LMNTRIX

BE THE HUNTER | NOT THE PREY

WHITE PAPER

RANSOMWARE PROTECTION, CONTAINMENT, AND RECOVERY GUIDE

2021

lmntrix.com

EXECUTIVE **SUMMARY**

The stark truth is that ransomware attacks are growing significantly in both volume and aggressiveness. Estimations are that attackers launch attacks worldwide every 11 seconds. The cost to global businesses of these attacks is estimated to reach $20 billion in 2021. This cost has grown more than fifty times the estimated cost impact seen in 2015. This staggering metric shows that ransomware is the fastest growing form of cybercrime, and the trend over the last three years shows the growth accelerating.

A key feature of ransomware is that it can be targeted at any business size, from the largest multinationals down to individuals. As a result, every system is vulnerable and can be seen as a viable target for attack. Traditionally ransomware attacks were focused on large organizations where a high financial ransom could be extorted. However, the trend is for attackers to target large numbers of small, less well-protected businesses more likely to pay a modest ransom. These more minor victims are more willing to pay, and the attacks are less likely to attract the attention of law enforcement organizations.

Ransomware is now a common attack vector for criminal enterprises seeking to extort businesses for financial gain. The technological capability of this malware variant has become pervasive and highly capable, able to penetrate stringent security controls through the exploitation of a weak point and quickly spread across systems. A successful infection will cause significant disruption to business operations for the duration of the active incident. Even the best backup and recovery plans take time to restore systems to a pre-infected state. However, ransomware attacks are evolving, so they no longer simply compromise data integrity and impact availability. The latest attack strategies include the exfiltration of data before encryption, followed by threats to compromise confidentiality by releasing the stolen data to the public or its sale to criminal enterprises for exploitation of any sensitive information. The ability to recover systems from backups is no longer sufficient to protect businesses from the impact of ransomware attacks. The focus must be shifted away from recovery to fast detection and effective response.

The key takeaway is that ransomware is becoming more common and more pervasive. The emergence of ransomware-as-a-service schemes enables any individual or group with criminal intent to launch an attack without the need for technical understanding of the attack mechanism. Anyone with basic computer skills and access to the internet access can launch an attack and take a share of any ransom paid. The groups providing the service make a lucrative income that can be invested in improving the ransomware, increasing its capabilities and success rate. Businesses need to take action if they are to stay one step ahead.

LMNTRIX's detection and response capabilities offer clients of all shapes and sizes an effective solution to the latest ransomware threats. The **LMNTRIX** Respond endpoint agent blocks malware and ransomware while the rest of its service stack offers tailored detection and response capabilities. The services detect ransomware at the earliest execution stage to minimize impact before the malware gets a foothold in compromised systems.

LMNTRIX
BE THE HUNTER | NOT THE PREY

CONTENTS

AN OVERVIEW OF **RANSOMWARE**

INTRODUCTION

Ransomware attacks are growing significantly. Incidents have been steadily rising since 2016 and now represent 10% of all reported security breaches. Last year, amid the Covid-19 pandemic, saw a marked increase in ransomware attacks against US-based organizations.The level of aggressiveness displayed by ransomware and its operators since 2018 has grown significantly. It has become so dynamic and volatile that a ransomware attack and subsequent recovery can cripple businesses both temporarily and permanently.These attacks include large volumes of low-value ransom demands against small companies and individuals as well as several multi-million dollar ransom demands against large organizations. All the while, attacks have evolved from the simple encryption of data to the theft and threats to publish.

RANSOMWARE BREACHES (PERCENT OF TOTAL INCIDENTS)

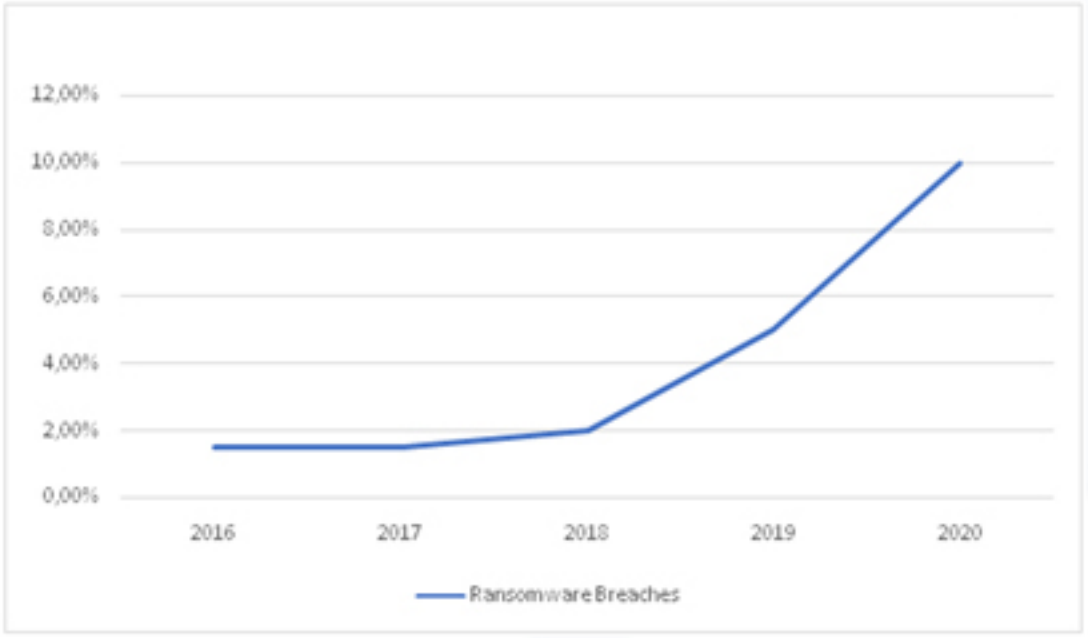


FIGURE 1 - INCIDENTS INVOLVING RANSOMWARE BREACHES

THE EVOLUTION OF RANSOMWARE

Ransomware is defined as malware that prevents users from accessing data or services on an infected system until a financial ransom is paid to restore access.The first recorded attack that employed this technique dates back to 1989. In this instance, the code known as the AIDS Trojan was delivered by the targeted distribution of computer floppy disks to delegates who attended the 1989 World Health Organization AIDS conference. The perpetrator, a fellow research scientist, disguised the malware as data related to the AIDS epidemic.This malware encrypted data on the victim's computer and demanded a ransom payment be sent by post to an address in Panama. The use of a weak encryption algorithm that security researchers were able to reverse made the attack unsuccessful. However, things have moved on quite a bit since this attack.

By the mid-2010s, attacks had moved on to the indiscriminate electronic distribution of malware that victims would receive and mistakenly or unwittingly execute to start the attack.

Email attachments and website links provided the primary mechanisms for delivering the ransomware. However, the malware had limited intelligence that restricted its ability to cause significant impact to infected systems or propagate between systems. As a result, the success rate for attacks was low.

It wasn't until around 2015 that attacks became sophisticated enough to generate significant financial benefits for attackers.

The focus now switched to targeted attacks on specific victims using hacking techniques to penetrate systems as the precursor to the use of ransomware. A hacking collective known as The GOLD LOWELL group was the first cybercriminal gang to use post-intrusion ransomware. Once they had successfully penetrated a network, they deployed the SamSam ransomware. By manually uploading and propagating the malware, attacks could be more successful and sufficiently destructive to persuade victims to pay a significant ransom. Other groups soon adopted this approach using the Ryuk, Defray, and BitPaymer code to extend attacks to include a ransomware element. But now, there is a new generation of ransomware code available. The following are the top ten reported infections in 2020, representing just over 65% of successful ransomware attacks.

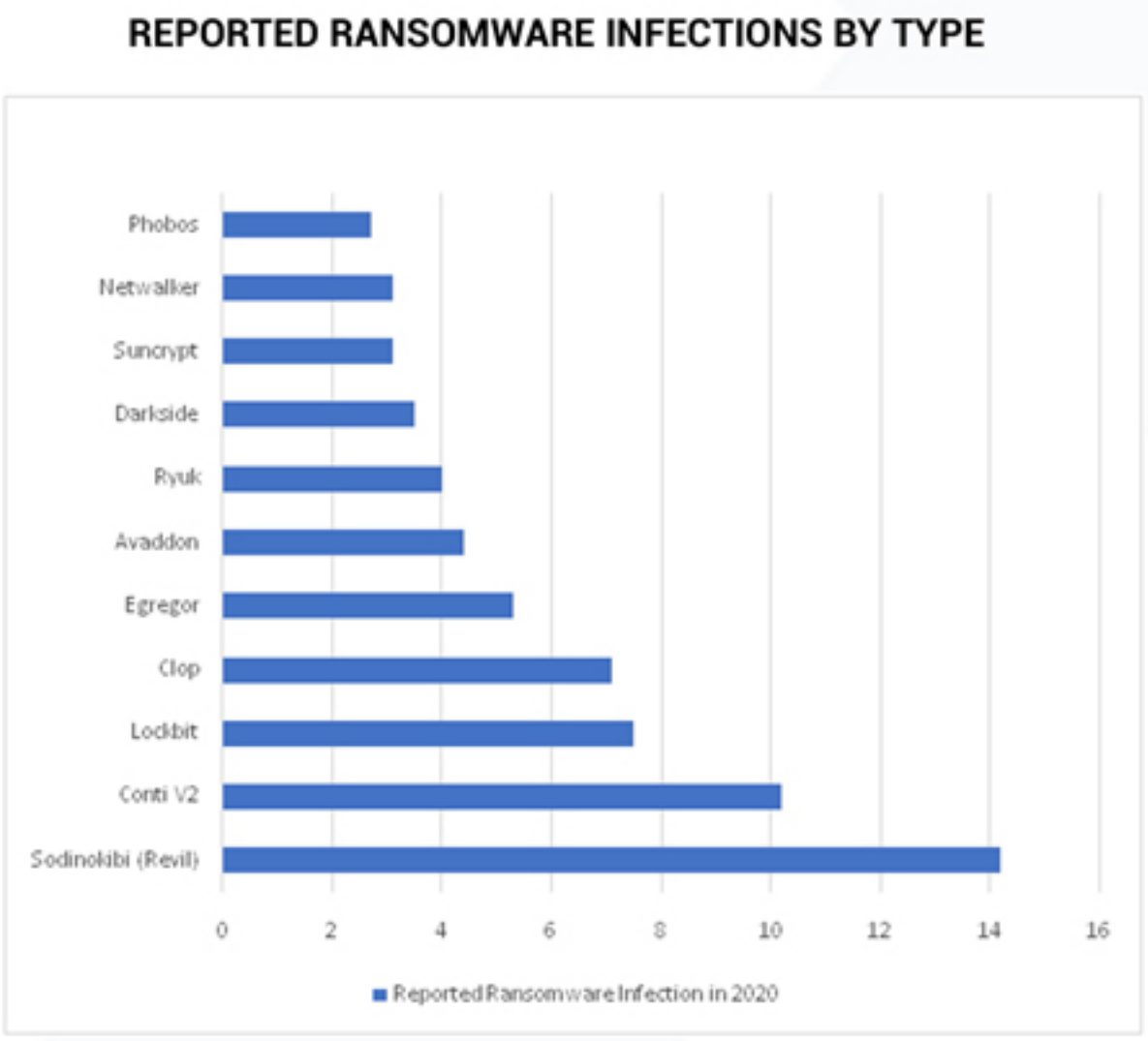


FIGURE 2 - REPORTED RANSOMWARE INFECTIONS BY TYPE

As each group became more successful and collected significant ransom payments, other groups and individuals were attracted to this attack method, including groups operating on behalf of some nation-states. This rapid growth amongst the criminal elements sparked the development of the ransomware-as-a-service (RaaS) business model. The successful ransomware creators provide less capable attackers with copies of their malware and the means to deploy it in return for a percentage share of all ransom payments. The benefits are financial income with little effort and less risk of payments being traced to the RaaS provider from the victims. The risks are shifted to those attackers undertaking the deployment. This move has opened up sophisticated ransomware as an effective attack option for hackers with little or no technical skills. These geographically dispersed individuals are much harder for law enforcement agencies to trace, making recovery of ransom payments significantly harder.

Ransomware is now a highly lucrative enterprise for malware writers and hackers able to gain access to systems. Criminal enterprises are willing to pay significant sums for software that delivers results. This market has driven the development of ever more technologically capable and highly pervasive malware to meet this need. This evolution has created a whole ransomware ecosystem where specialist skills are brought together to deliver an end-to-end attack on behalf of a criminal group.

TARGET	RANSOMWARE TYPE	RANSOM PAID
CWT GLOBAL	Ragnar Locker	**$4.5 MILLION**
COLONIAL PIPELINE	DarkSide	**$4.4 MILLION**
BRENNTAG	DarkSide	**$4.4 MILLION**
TRAVELEX	Sodinokibi	**$2.3 MILLION**
UNIVERSITY OF CALIFORNIA SAN FRANCISCO (UCSF)	NetWalker	**$1.14 MILLION**

FIGURE 3 - TOP RANSOMS PAID

THE CURRENT STATE OF PLAY

Ransomware is now a common attack vector for criminal enterprises looking to extort money directly from businesses. From the attacker's point of view, this technique requires little effort, technical know-how, and resources to accomplish. However, the emergence of RaaS means that anyone in any geographical location armed with a computer and an internet connection can launch attacks.

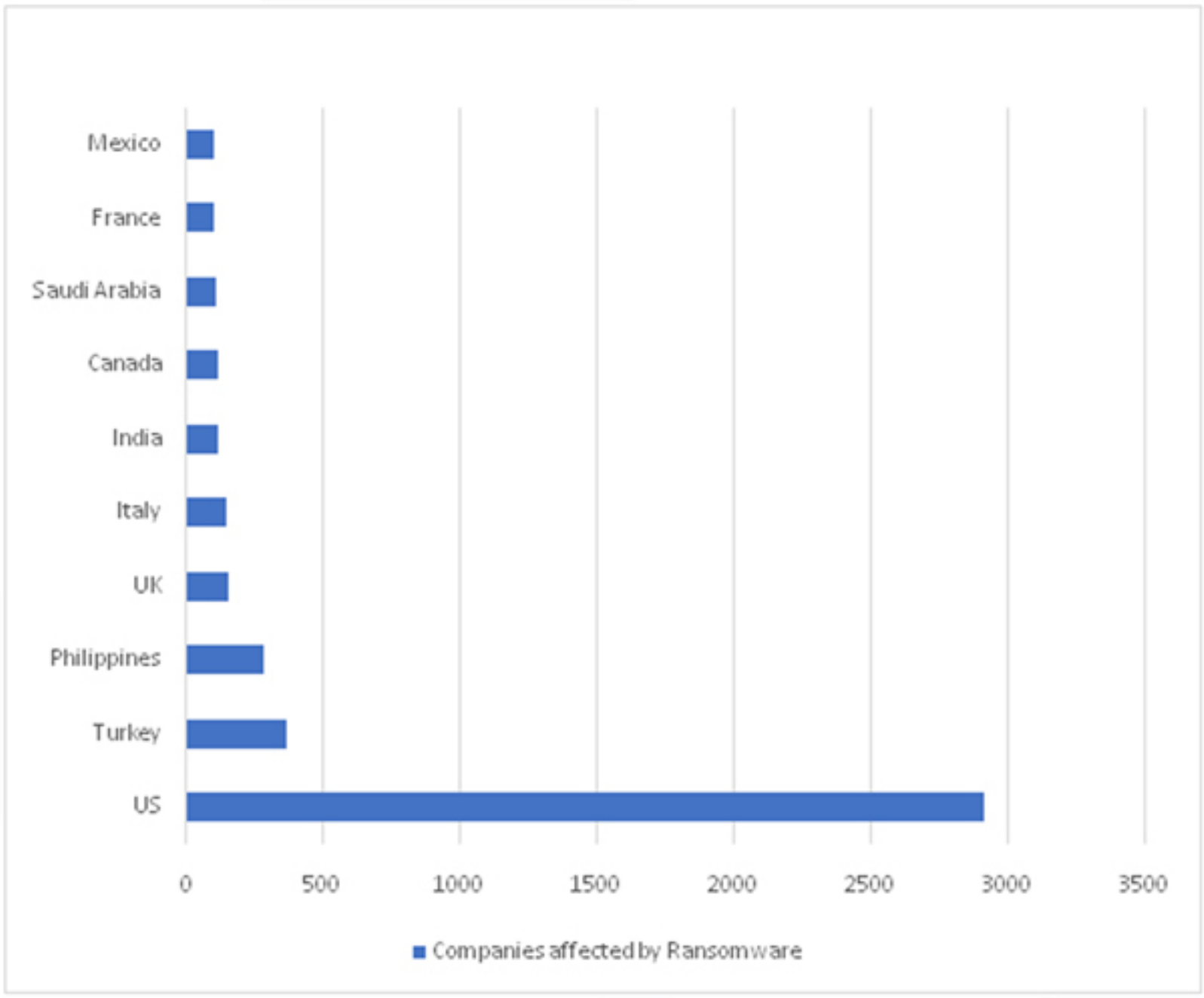


FIGURE 4 - RANSOMWARE INFECTIONS BY COUNTRY

In almost all cases, ransom payments are required to use cryptocurrency to obfuscate the financial trail back to the perpetrator.The unregulated nature of cryptocurrency transactions and the low adoption rate of this technology made it easy for such payments to be converted to cash or other assets reasonably anonymously. However, the investigative capabilities of law enforcement agencies have significantly become enhanced in recent years, providing the ability to track the movement of large cryptocurrency transactions.This ability is making it more difficult for criminal enterprises to hide the flow of money. As a result, while the collection of payments remains straightforward, the criminals are finding it increasingly difficult to realize the financial value of the cryptocurrency without attracting unwanted attention.This factor is driving a focus on collecting large volumes of small transactions across several different cryptocurrencies that are easier to obfuscate among other legitimate transactions.

FIGURE 5 - RANSOMWARE ATTACK SUCCESS RATES

Increasingly, attackers were seeing their efforts go to waste as victims were able to restore infected systems. The growth of backup solution providers and specialist recovery businesses has seen a significant increase in the recovery capabilities of organizations that used to be vulnerable to ransomware attacks.In response, the attacks have evolved to counter the increased use of such data backup solutions to mitigate such attacks by exfiltrating sensitive information and using the threat of releasing this information to encourage payment.This 'name and shame' attack is the latest method to improve success rates when faced with defense improvements.

The following statistics for ransomware that employs a 'name and shame' strategy are derived from postings made by attackers to leak sites and represent the number of victims who did not pay a ransom.

RANSOMWARE NAME	DATE OF FIRST KNOWN NAMING	PERIOD OF OPERATION (DAYS)	NUMBER OF NAMED VICTIMS
CLOP	February 2019	871	65
REVIL	May 2019	782	259
SNATCH	May 2019	16	6
DOPPELPAYMER	July 2019	720	200
NETWALKER	September 2019	509	144
PYSA	October 2019	619	189
LOCKBIT	October 2019	611	9
CONTI	November 2019	570	417
MAZE	December 2019	334	266
RAGNAROK	January 2020	537	33
AKO	January 2020	181	9
RAGNARLOCKER	February 2020	503	27
NETFILM	March 2020	464	40

RANSOMWARE NAME	DATE OF FIRST KNOWN NAMING	PERIOD OF OPERATION (DAYS)	NUMBER OF NAMED VICTIMS
NEMTY	March 2020	1	1
SEKHMET	March 2020	103	6
AVADDON	June 2020	373	182
RANSOMEXX	June 2020	369	21
MOUNT LOCKER	July 2020	355	20
DARKSIDE	August 2020	285	99
RANZY	August 2020	307	3
SUNCRYPT	August 2020	300	22
EGREGOR	September 2020	103	206
EVEREST	December 2020	202	39
CUBA	December 2020	202	9
BABUK	January 2021	168	43
ASTRO TEAM	March 2021	111	16
PROMETHEUS	March 2021	85	37
SYNACK	March 2021	85	6
LV	April 2021	73	40
MARKETO	April 2021	69	32
NONAME	April 2021	54	6
XING	April 2021	53	18
LORENZ	April 2021	53	17
GRIEF	May 2021	25	15
PAYLOAD BIN	May 2021	21	2

FIGURE 6 - NAME AND SHAME METRICS

It is expected that the use of 'name and shame' ransomware will continue while it remains profitable. However, ransomware is constantly evolving, and a new attack method is expected to emerge.In addition, improving law enforcement capabilities and better defenses against attacks will eventually force a change in direction.The trick for businesses is to stay one step ahead to minimize the chances of attack while also being fully prepared to detect and respond if and when an attack occurs.

THE INFECTION PHASE

A ransomware attack starts the same as any typical malware attack.The attackers seek a mechanism to install their ransomware to a target system undetected.They are helped by the many options available, depending on their capabilities and the nature of the target.

- Using a phishing email or other communications medium includes a link to a website that hosts malware that the attacker hopes will not be detected. Then, the target's systems will download and execute.

- Using stolen or deduced access credentials to gain access to a system to install and execute malware.

- Using social engineering techniques to persuade a legitimate system user to allow access using a desktop sharing application, allowing the attacker to install and execute malware.

- Using traditional network attack techniques to exploit a weakness in security controls to gain access to a system to install and execute malware.

- Using malvertising techniques to hijack advertising delivered by legitimate websitesto deliver adverts that link to malware that the attacker hopes will not be detected. The target's systems will download and execute.

- Secondary infection techniques are also being used where criminal organizations utilizing ransomware obtain access to systems that unknowingly have been previously infected with malware by a group or individual.

This task is more straightforward for the attacker thanks to the availability on the dark web of stolen access credentials and details of individuals and businesses who have previously fallen victim to attacks. Thus, for a relatively modest price, attackers can gain access to all the tools necessary to launch an attack.

THE ATTACK PROCESS

Once a system has been compromised with malware, the attack process will begin.Simple forms of ransomware would simply encrypt all the files on the infected device and send a message containing the randomly generated encryption key back to the attacker.Usually, the keys are sent to a server controlled by the attacker, located in a territory with no regulator controls where anonymity can be guaranteed.

Ransomware has since evolved to be more sophisticated and persuasive.Typically, the initial malware acts as a loader for more complex applications that undertake surveillance and intelligence gathering activities.The goal is to spread across as many connected systems as possible, collecting credentials to increase access permissions and identify valuable information.

Now, ransomware will typically seek to exfiltrate as much information as possible. Data is transferred discretely from the infected systems back to the attacker-controlled server.This tactic has two benefits. Firstly, the threat to release the information can incentivize the victim to pay the ransom demand in cases where recovery from a backup is a viable option. Secondly, the information has a potential value, and a marketplace for the sale of such information exists on the dark web. The downside for the attacker is that the exfiltration of large volumes of data may reveal that the attack is underway before the encryption of the data commences.This red flag provides an opportunity for the target to detect an attack in progress and halt it.

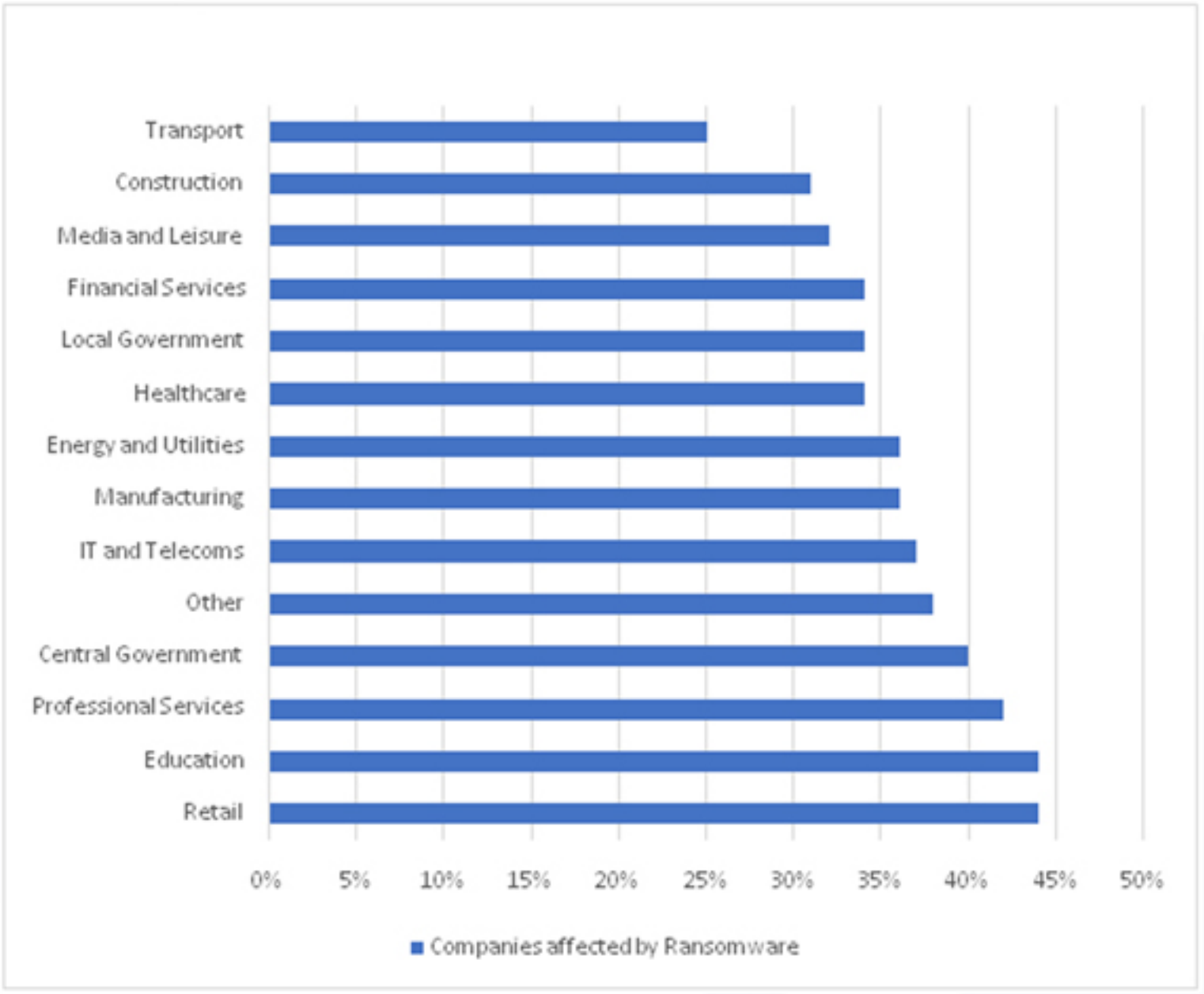


FIGURE 7 - RANSOMWARE ATTACKS BY SECTOR

Ransomware will also perform additional functions to prevent or complicate recovery efforts. For example, the LockerGoga malware covered in one of the following case studies will attempt to disable all registered accounts on an infected system by changing the password and forcing a log-off action for each account.This feature makes restoring systems more challenging, necessitating a complete rebuild rather than the restoration of data files.

The trend in ransomware development is for a mechanism that enables an attacker to broadly target any data that will impact the target business's operations to increase the likelihood that a ransom will be paid.

ATTACK PSYCHOLOGY

The majority of ransomware attacks are targeted based on geographic location and industry sector. Attackers will most often target businesses relying on access to digital information to undertake their business operations, specifically those likely to have highly sensitive information stored in unencrypted form.

Targeting data-centric companies in verticals such as financial services, healthcare, and educational services in affluent regions such as North America and Europe will tend to deliver the greatest financial rewards. However, significant levels of attacks are also observed in some Asian regions where the motivation is skewed towards interference to rival businesses operations rather than extortion. In these cases, ransomware is leveraged towards deliberate disruption rather than the collection of a ransom.

Attacks also tend to focus on small to medium-sized businesses where security controls may be less rigorous due to budgetary constraints and limited access to the necessary expertise.

Countries whose first language is widely spoken, such as English or Spanish, tend to be more popular targets due to the ease of crafting compelling phishing content or performing successful social engineering. By contrast, Japan has one of the lowest incidents of ransomware attacks of the more affluent nations due to the complex nature of its language.

PERCENTAGE OF COMPANIES AFFECTED BY RANSOMWARE BY COUNTRY

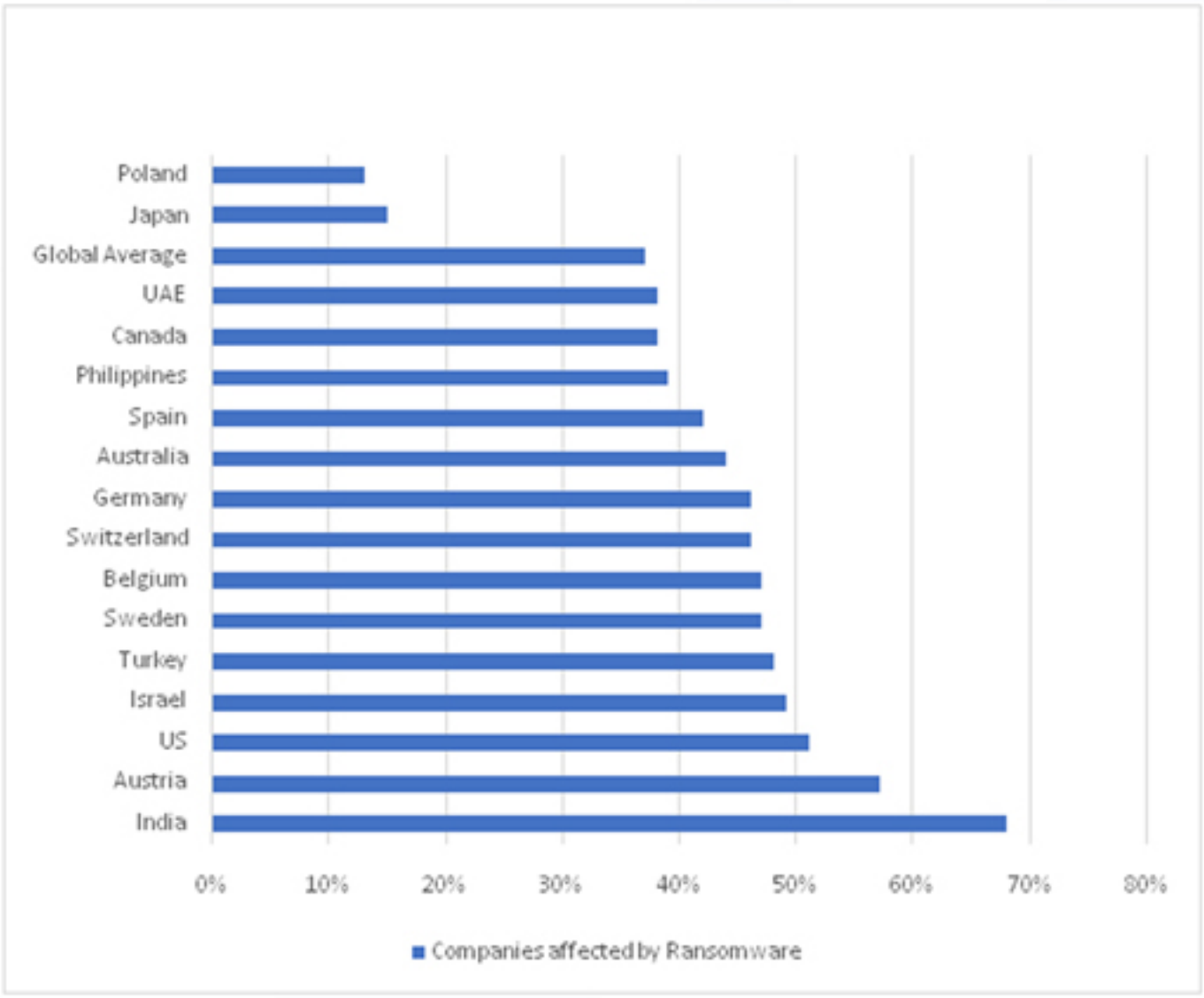


FIGURE 8 - RANSOMWARE AFFECTED COMPANIES BY COUNTRY

Interestingly, ransomware has been analyzed and found to exclude specific targets explicitly. For example, the ransomware used for the attack on the US Colonial Pipeline was coded not to execute on any system where the operating system language was set to Russian.

Recent intelligence has also revealed that organized attackers may prefer to target businesses with cyber insurance on the basis that they are more likely to pay a ransom.They have been seen to conduct cyberattacks on cyber insurance providers, presumably to gain access to client lists.This demonstrates the sophisticated intelligence behind ransomware attackers.

CONSEQUENCES OF RANSOMWARE INFECTION

A successful infection will cause significant disruption to business operations for the duration of the active incident.This impact will often go beyond the unavailability of infected systems. In all the case studies, you will see that systems' intentional and controlled shutdown causes the most disruption.This impact is experienced due to measures intended to prevent the spread of ransomware and limit damage. Unfortunately, victims often mistakenly switch off systems as an initial reaction when they should hibernate a system after ransomware infection to enable retrieval of data from memory and storage.

The time required to restore operations for systems that have been shutdown fully can be significant, raising the question of whether this was the most practical action. Once known infected systems have been restored, any systems that were shutdown must be checked to ensure they are infection-free before restarting operations. In the case of industrial processes, restarting a system can take days or weeks, restoring operational processes can take months.The following statistics demonstrate how the cost of remediation can dwarf the average ransom payout.

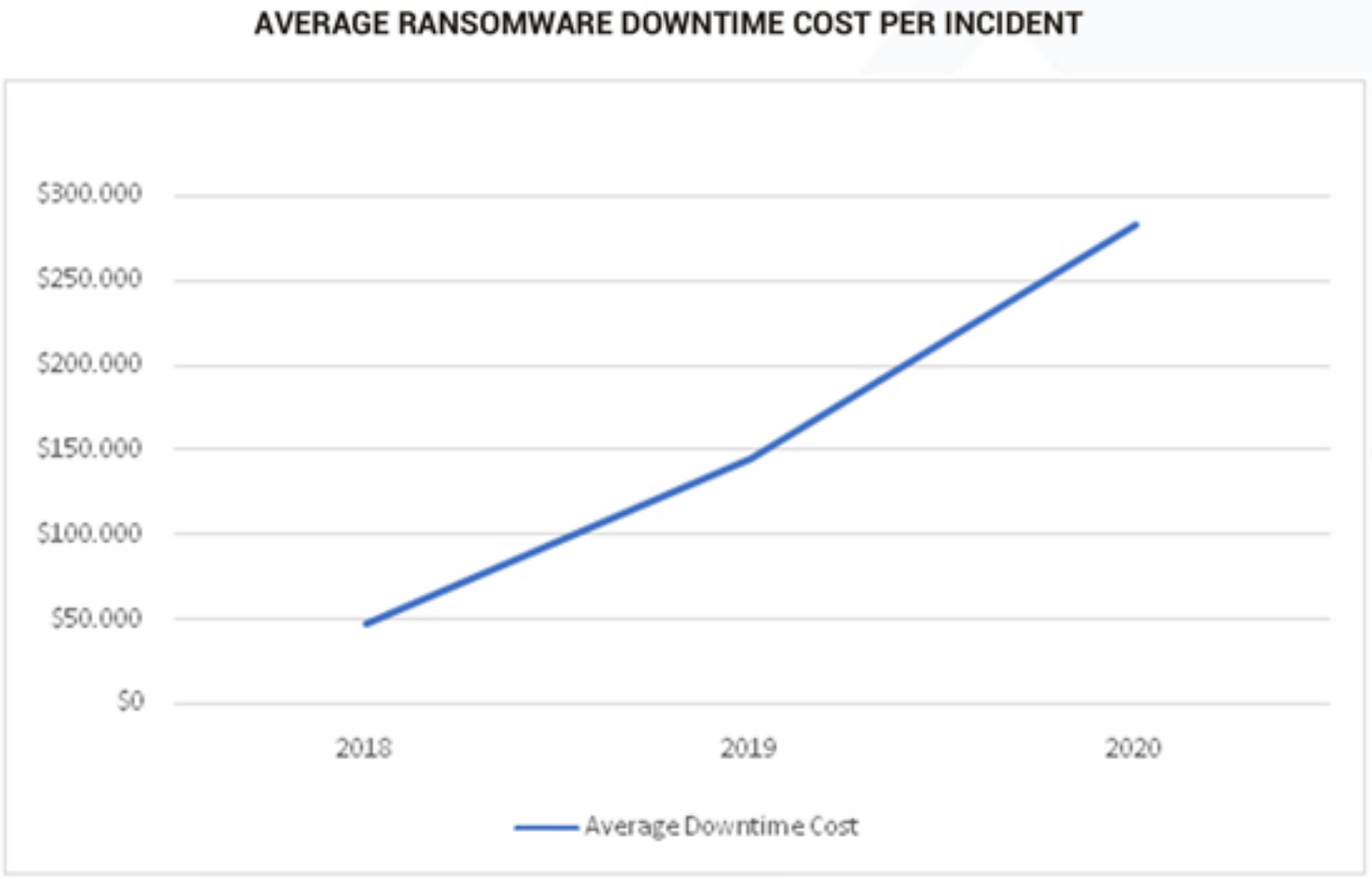
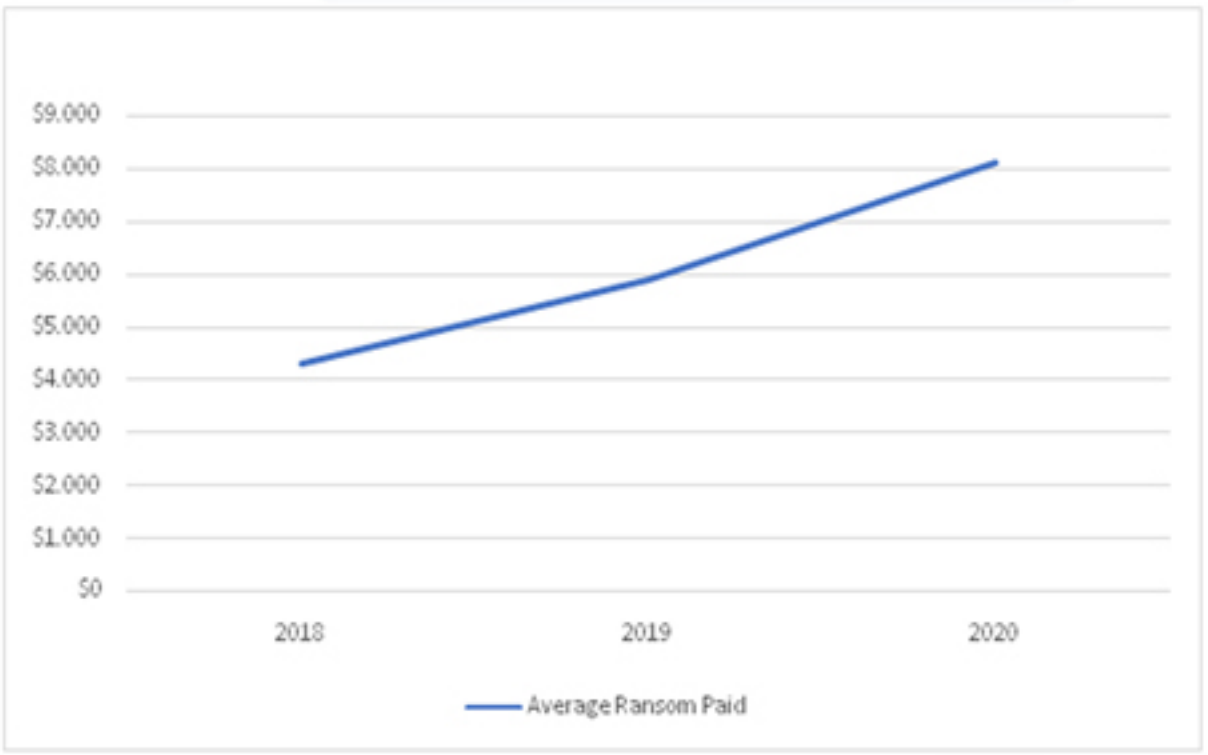
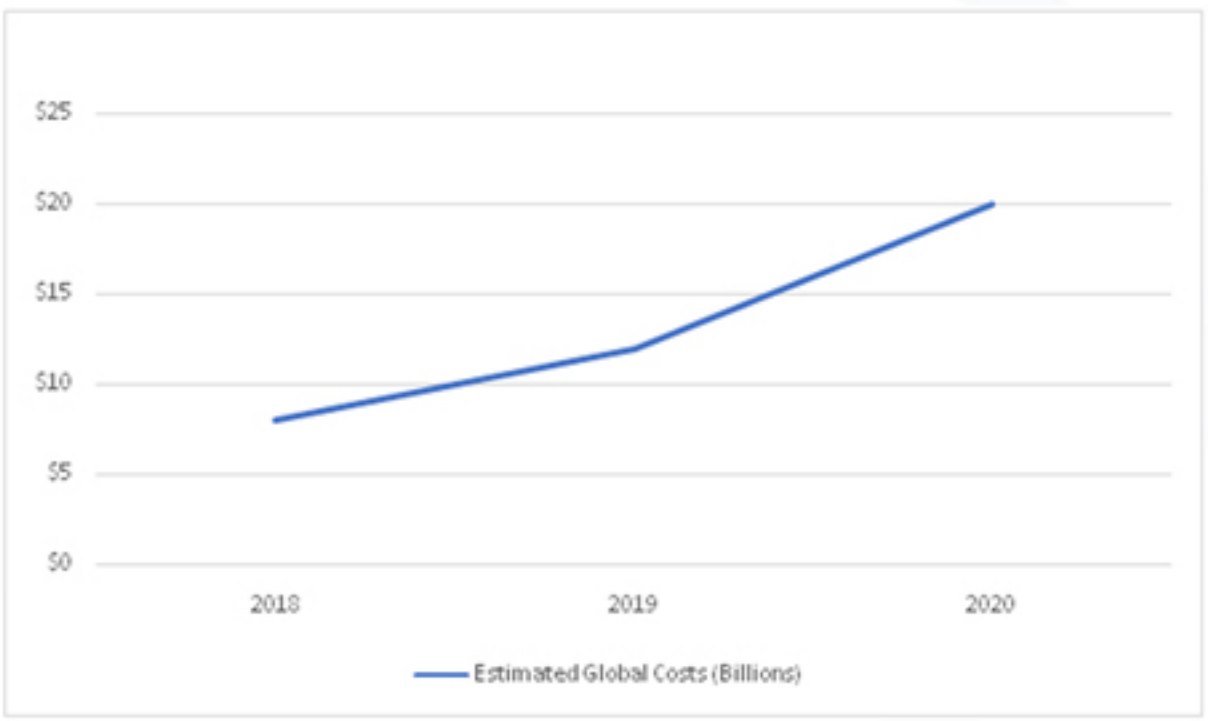


FIGURE 9 - AVERAGE RANSOMWARE DOWNTIME COST PER INCIDENT



AVERAGE RANSOM PAID PER INCIDENT

FIGURE 10 - AVERAGE RANSOM PAID PER INCIDENT



ACCUMULATIVE GLOBAL COST OF RANSOMWARE

FIGURE 11 - ACCUMULATIVE GLOBAL COST OF RANSOMWARE

Recent intelligence has also revealed that organized attackers may prefer to target businesses with cyber in a simple system that benefits from an effective backup and recovery plan will take a finite time to restore systems to a pre-infected state. This period is when business operations are disrupted, directly resulting in a financial impact. Identifying infection early enough in the attack lifecycle to prevent data compromise is the only security control that precludes such disruption.

However, as we've seen, ransomware attacks are evolving. They no longer simply compromise data integrity to affect system availability. The latest attack strategies include the exfiltration of data before encryption, followed by threats to compromise confidentiality by releasing the stolen data to the public or its sale to criminal enterprises for exploitation of any sensitive information. The ability to recover systems from backups is no longer sufficient to protect businesses from the impact of ransomware attacks. This threat evolution reinforces the message that the focus must be shifted from recovery to fast detection and effective response.

RECOVERY FROM INFECTION

The attacker intends that the victim should pay a ransom and, in return, receive an application that will decrypt the affected data to restore the systems to the pre-infected state. Indeed, there is still a significant percentage of victims that follow this path.

The official government advice is never to pay a ransom on the grounds that it simply perpetuates attacks, not only incentivizing criminal organizations to carry on using ransomware as an attack vector but also providing funds to enhance and extend the capabilities of the ransomware.

There are other reasons why organizations should not pay a ransom. Firstly, there is no guarantee that the attacker will honor their promise to provide a decryption mechanism. Once they have received payment, they may simply disappear. Secondly, there is no guarantee that the decryption mechanism will work. Flaws may exist in the encryption or decryption code; the quality of the code is unlikely to be reasonable given its purpose. Thirdly, the victim is paying a criminal with hacking capabilities to download and execute an application of unknown providence. Finally, the application that decrypts the files will have a very high probability of including other malware. All things considered, the risks are enormous.

The alternative to paying a ransom is to restore systems from backups. While this may be time-consuming, it eliminates the risks associated with using a decryption tool.

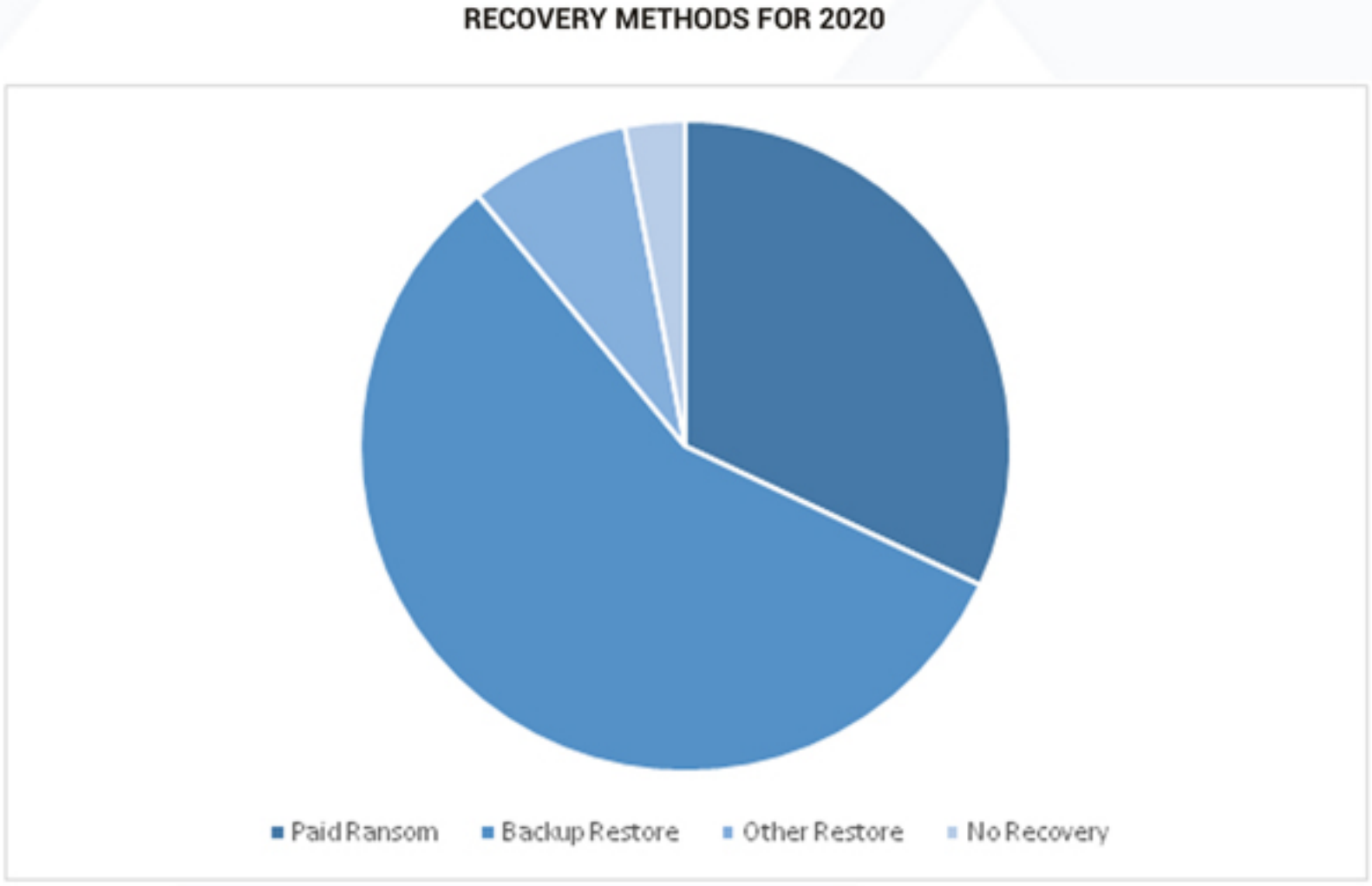


FIGURE 12 - RANSOMWARE RECOVERY METHODS

BUILDING EFFECTIVE DEFENSES

Ransomware has evolved to utilize sophisticated, persistent attack vectors to deliver malware, creating a challenge for organizations looking to build effective defenses. Unfortunately, technological controls alone are not sufficient.

Traditional security controls rely on the static analysis of data looking for known signatures to detect and block known threats. Anti-virus software, next-generation firewalls, and intrusion detection systems all use this approach to detect known threats and anticipate new threats. Unfortunately, attackers have the benefit of time to test the implemented security controls to identify exploitable weaknesses. Once a hole in the defenses is identified, the attack can commence. All it takes is a delay in implementing a security patch or updating virus signatures to give attackers a window of opportunity.

To counter this advanced persistent threat, organizations need to employ a combination of technology controls with intelligent monitoring and robust threat intelligence.

- Defenses need to be quickly updated to keep pace with evolving threats and newly identified vulnerabilities.

- Monitoring needs the capability to detect and recognize novel threats before they can generate an actionable attack vector.

- Monitoring needs the capability to detect obfuscated communications from systems to the outside world that can indicate unauthorized data exfiltration or malware command and control processes.

- Threat intelligence needs to identify potential weaknesses in security controls and provide mitigating actions before exploitation can occur.

The majority of ransomware attacks begin with an external attack on an endpoint. Therefore, endpoint security and user awareness are critical components in the multi-layered integrated defense suite needed to provide adequate security controls in today's threat environment.

Advanced threat detection and response provided by technological controls supported by actionable threat intelligence will provide the best defense against ransomware.

RANSOMWARE **CASE STUDIES**

COLONIAL PIPELINE ATTACK

The most recent high-profile ransomware attack was undoubtedly the disruption to the Colonial Pipeline in May 2021. The Colonial Pipeline is the largest refined oil pipeline network in the USA, over five and a half thousand miles in length, transporting two and a half million barrels of gasoline, diesel, and jet fuel from refineries in Texas up the East Coast, ending in New York City. The affected pipeline connects 29 refineries with 267 distribution terminals, accounting for up to 15% of the daily oil capacity in the US. The attack resulted in the controlled shutdown of the pipeline for six days. With the pipeline providing around 45% of the fuel used in the East Coast states, this led to significant shortages and caused knock-on effects, including changes to flight schedules and price rises at affected automotive filling stations.

The ransomware affected the billing systems of Colonial Pipeline's operator, and the perpetrators also claimed to have stolen around 100 gigabytes of data that they threatened to release. The computer systems were shut down immediately following detection of infection, preventing further spread of the ransomware. However, there was no evidence that the operational systems for control and monitoring of the pipeline were compromised. As a result, the pipeline operator decided to pay approximately $5 million ransom and shut down the pipeline while restoring the compromised systems.

There was a problem in the fact that the tool supplied for the decrypting process was so slow that it turned out that a complete restoration from backups needed to restore the affected systems was quicker. If backups were not available, the disruption would have lasted longer, assuming that the decryption tool worked correctly. Given that a criminal organization provided the tool, trusting that it would work and not introduce other malware is a significant risk to take.

Even with the successful restoration from backups, the pipeline was shut down for six days and then took two more days to return to regular service. Then followed a period where the pipeline had to fulfill regular demand and provide additional oil products to resolve the shutdown period's shortfalls.

The attack was traced to the DarkSide criminal group based in Russia. One giveaway to their identity was a line in the ransomware software preventing installation on any device where the operating system language was set to Russian. As a result of the attack, the authorities in an unnamed country seized servers used by this group. Consequently, the US Department of Justice recovered around 85% of the ransom. However, due to a significant drop in the value of bitcoins in the period between the ransom being paid and subsequently recovered, the recovered funds represented around 50% of the ransom. It is estimated that in the period from August 2020 to May 2021, when DarkSide was active, they successfully extorted more than $90 million in ransom payments.

DarkSide's approach was to enact multi-faceted extortion involving data exfiltration (theft of sensitive information) and data encryption (compromising information availability). This tactic necessitates the victim paying a ransom to decrypt data and incentivizing payment to prevent releasing their data to the general public or the dark web. Additionally, this approach discourages victims from simply relying on data restoration from backups to re-establish the availability of information.

DarkSide began operations in August 2020, focused on ransomware infection of Windows-based systems. Once their malware is introduced into a target system, it commences a passive process of gathering all credentials and unencrypted documents it finds and sending this data to a server operated by the group. Once access to Windows domain credentials is obtained, the ransomware application is deployed to all accessible devices to encrypt all stored data actively. This technique offers two potential revenue sources, a ransom to provide a tool to decrypt data and a ransom to keep the stolen documents private. This approach is particularly successful in targeting a commercial organization with unprotected commercially sensitive information stored on its systems.

The conscious decision to shut down the operational systems to prevent the malware from spreading from the financial systems may have prevented more significant disruption. However, this action came at the price of considerable business disruption with the financial and reputational hit that it brought. It also disrupted end customers and necessitated a federal response to mitigate disruption through alternate shipping mechanisms.

While DarkSide reportedly stated that their aim was not to cause disruption, this event clearly showed the vulnerability of industrial systems to cyberattack. Additionally, a more sophisticated attack targeted at the industrial control systems could have caused significantly more significant disruption or even environmental damage by attacking the physical infrastructure.

The network infrastructure was designed to segregate the critical control systems onto a private network, isolated from the internet and other company systems. The financial systems were part of the non-critical systems that had internet connectivity through which the ransomware entered the network. In theory, the ransomware attack would have resulted in the temporary loss of day-to-day business functions. At the same time, the systems were restored, with no disruption to the operations side of the business. The problem was that the air gap isolating the critical control systems had been inadvertently bridged when an unauthorized internet-connected device was added to the network. The investigation of the networks following the detected infection of the non-critical systems identified the compromise to the critical network, which meant that the business could not be sure that the malware had not crossed over to this vital network. This uncertainty led to the decision to shut the critical network down while investigations continued and malware removed from all systems. A simple mistake had compromised carefully planned network security controls.

The initial attack vector employed by this group was a combination of brute force password attacks, phishing attacks that included a link to a malware downloader, and the attempted exploitation of a SQL injection vulnerability that was publicly disclosed in April 2021.

WANNACRY

Probably the most widespread ransomware attack occurred in May 2017 with the release of the WannaCry malware. What made this attack different is that the malware was a worm, software that self-replicates with the intent of installing a copy on every connected system that it can access. Once installed, the ransomware aspect of the software would then be ready to come into play when activated.

The malware was developed by the North Korean-based Lazarus Group and worked by exploiting older versions of the Windows operating system via a vulnerability that had been publicly disclosed a year earlier, in April 2016. The first detected infection was recorded in Asia in April 2017. In just four days, it is estimated that over a third of a million devices were infected across one hundred and fifty countries.

The ransomware operates by encrypting files on the affected computer, primarily targeting documents, videos, and pictures. It then displays a message providing details of how to pay the ransom and how much to pay. The display included two countdown timers; after three days, the required fee doubled at the expiration of the first counter. At the expiration of the second counter, after seven days, the malware would delete the encrypted files. This approach was intended to incentivize victims to pay the ransom quickly before a thorough investigation of the nature of the ransomware could be conducted. Subsequent events highlighted the reasoning behind this approach.

First, an analysis of the ransomware software by a security researcher identified the presence of a kill-switch. The simple registering of a specific domain name would disable the ransomware from executing and prevent further infections.In response to the discovery and activation of the kill-switch, a modified version of the malware was released that removed the kill-switch function.

Second, the ransomware created an RSA key to encrypt the files and then sent this key back to a server controlled by the attackers to decrypt the files once the ransom had been paid. A security researcher discovered a mechanism for retrieving the RSA key from the malware, allowing decryption without ransom payment.

Third, the rapid rollout of patches for vulnerable computers and updates for anti-virus software definitions prevented infection.

These three actions significantly reduced the effectiveness of the WannaCry ransomware attack after four days, effectively halting the attack. In the end, only around $100 thousand ransom was paid. However, the time and effort needed to restore the infected computer systems was considerable, estimated to be $ billion.

One of the most significant impacts of this ransomware attack was on the British health system. The IT systems of the health care providers were typically composed of older equipment running older versions of Windows operating systems. Each hospital, healthcare trust, and doctor's surgeries typically manage their local IT systems in isolation, often without access to full-time IT administrators. These systems are all connected to a national IT system backbone that provides critical services. When WannaCry infections were first seen in individual healthcare IT systems, health care workers used social media to communicate the news and warn other users. As a result, a significant number of users decided to protect their systems by disconnecting them from the backbone network. The consequence of this action was an immediate loss of the central digital services that they relied on. This action impacted patient care and resulted in around seven thousand canceled hospital appointments, disruption to diagnostic services, and impacting secondary care are resources focused on more critical patients.

80 out of 236 hospital trusts across England were affected, 34 of which had systems infected with the ransomware while the remaining 46 were not infected but reported disruption. In total, over a thousand pieces of diagnostic equipment were infected by the ransomware. This figure represents a minute fraction of the total computer-based equipment used across the health service. In addition, none of the affected trusts has applied the relevant security patch that would have prevented infection, despite having been required to do so. The prominent disruption was caused by a lack of availability of electronic patient records and loss of access to clinical systems. The most severe consequences were that operations had to be canceled, and many accident and emergency centers had to close while the disruption lasted.

NORSK HYDRO

One of the world's largest aluminum producers, Norsk Hydro, suffered a ransomware attack in March 2019. The attack started when an employee opened an infected email disguised as a communication from a trusted supplier. This action installed malware that allowed the attackers to probe the infected systems for weaknesses and opportunities for lateral movement and privilege escalation

When the ransomware attack was launched, 22,000 Windows-based computers located across 170 sites in 40 countries were affected by the LockerGoga malware. This malware is designed not to trigger network defenses and evade sandbox and virtual machine-based controls. Instead, this software encrypts files and attempts to disable user accounts by changing passwords and logging users off the systems. This action created a significant challenge for removing the infection and restoring systems.

The company responded by shutting down the IT systems and switching to manual operations to maintain as much of the business and production functions as possible. As a result, some production lines had to halt, but others could continue using manual controls. In some instances, retired workers came in to help, bringing their knowledge of pre-computerized control methods.

The main feature of this attack was that Norsk Hydro did not engage with the attackers; there was no ransom paid, indeed no negotiation. Instead, the reversion to manual processes brought the company time to restore all the affected systems. This process lasted a few months and had a financial impact of around $50 million, including the offset from cyber insurance payments.

The other key aspect to this attack is that the company adopted an open and transparent attitude from day one, with regular press briefings, progress reports, and even producing video tutorial material. This response has provided a valuable learning opportunity for other organizations to see how to recover from a ransomware attack at a time when a significant number of infected businesses turn to brokers to secretly pay ransoms, with holding information from customers, suppliers, the public, and shareholders. Unfortunately, this practice encourages the proliferation of ransomware attacks and has led to the appearance of RaaS as a revenue stream for criminal enterprises.

ZERO COST **STRATEGIES**

There are many practical security measures that any organization can take to reduce its exposure to the risk of a ransomware attack.

PROTECTION PRACTICES

SECURITY AWARENESS

Users continue to represent a significant vulnerability to organizational security. When it comes to phishing attacks to launch a ransomware attack, the advantage is with the attacker. It only takes one user out of thousands to click a link or open an attachment for the attack to start. The median click rate for phishing simulations is typically a few percent, and anecdotally the click rate for actual phishing attacks is higher.

Practical user training with regular refresh sessions is the only effective defense for stopping phishing attacks once thee mail has reached the user's screen. Unfortunately, users are inherently fallible, particularly when placed under pressure to act.

CONTENT FILTERING

The best method for stopping phishing attacks is preventing content with suspicious links or malware-laden attachments from reaching users. Content filtering on emails and website access will effectively prevent users from being exposed to the risk of phishing.

A practical method of minimizing exposure to malicious online content is using strict allow lists that limit users to accessing only those services, websites, and web apps that have been assessed as safe. Blocklists are simpler to set up but are far less stringent and more effortless for an attacker to bypass.

EXECUTABLE AND PRIVILEGE CONTROLS

Central administration of application control functionality can be used to impose limits such that only programs and services on an allow list may execute. This approach can ensure that un authorized executables cannot run, limiting the options available for ransomware to execute.

Similarly, allow lists for access protection mechanisms can be used to define which services and processes are authorized to operate with privileges access to the system, ensuring unknown or unauthorized processes have limited access.

FILE ACCESS CONTROLS

Central administration of access control policies can be used to impose limits such that only programs and services on an allow list may access or change specific file types. This control can ensure that un authorized executables cannot alter files or exfiltrate data.

NETWORK ACCESS CONTROLS

Central administration of network access can be used to block access to anonymous Internet communication systems and specific networks such as Tor to prevent ransomware from communicating back to its host server. In addition, where proxy and gateway appliances are used, these should be configured to identify and block known ransomware control server traffic.

MINIMIZING VULNERABILITIES

Keeping operating systems and applications up to date with the latest security patches and software updates will reduce the number of exploitable weaknesses in a system. All software must be fully supported any end-of-life systems or unsupported applications should be replaced as a priority.

DISABLE MACROS

By default, macros in office documents should be disabled unless the macro is known to be safe. Typically, macros are disabled by default and require user action to enable, which will necessitate user awareness training to ensure macros cannot be exploited by attackers to introduce ransomware.

MINIMIZING PRIVILEGES

The principle of least privilege should be applied to ensure users are only given the minimum rights needed for their regular duties. This control includes access to services and stored data. This approach will limit the potential impact should attackers compromise that user's account.

DIVIDING DUTIES

For processes that can potentially have significant consequences, such as implementing a critical business operation, consider dividing duties such that no single user can perform the complete end-to-end process. Instead, impose rules that permit one user to execute part of the process and require an independent user to complete the process. This approach can prevent any compromised user account from completing a potentially damaging operation.

DUAL OPERATIONS

The use of dual operator policies is commonplace for initiating financial transactions or granting privileged access to systems. Actions by two separate users are required before a process can proceed. This approach will prevent a compromised user account from completing an operation that may significantly affect the business.

SANDBOXING SUSPICIOUS PROCESSES

Systems should be configured to identify and label processes as suspicious based on preset criteria such as prevalence, age, and behavior. Such processes should be sandboxed to isolate them from the operational systems until they have been proven to be safe.

WINDOWS SECURITY CONTROLS

Windows-based systems represent a significant percentage of target systems due to the availability of ransomware and known exploitation techniques. The following security measures will reduce the exposure of such systems to the risk of a ransomware attack.

NETWORK CONFIGURATION CONTROLS

Server Message Blocks (SMB) are commonly exploited by ransomware as a communications channel between systems. They provide trust relationships that can be used to deploy and execute code automatically. Therefore, the scope of authorized communications should be restricted to a minimum to reduce the opportunity for exploitation by ransomware code. For example, endpoint to endpoint communications can be limited while supporting the Domain Controller and File Server communications to endpoints necessary for normal operations.

Transmission Control Protocol (TCP) Port 445 utilized by SMB should not be left open on internet-facing systems as this provides an entry point for malware. Regular scanning of all public IP addresses for this open port can help minimize the ability of attackers to gain entry to a system.

The recommended Group Policy settings are to block all inbound connections on public and private profiles and only allow inbound connections for the domain profile that match prescribed rules.

Group Policy Setting Path:

ComputerConfiguration > Policies > WindowsSettings > SecuritySettings > WindowsFirewallwithAdvancedSecurity

PROFILE SETTING	FIREWALL STATE	INBOUND CONNECTIONS	LOG DROPPED PACKETS	LOG SUCCESSFUL CONNECTIONS	LOG FILE PATH	LOG FILE MAXIMUM SIZE (KB)
Domain	On	Block all connections that do not match a preconfigured rule	Yes	Yes	%systemroot%\system32\LogFiles\Firewall\pfirewall.log	4,096
Private	On	Block All Connections	Yes	Yes	%systemroot%\system32\LogFiles\Firewall\pfirewall.log	4,096
Public	On	Block All Connections	Yes	Yes	%systemroot%\system32\LogFiles\Firewall\pfirewall.log	4,096

FIGURE 13 - WINDOWS FIREWALL RECOMMENDED CONFIGURATION STATE

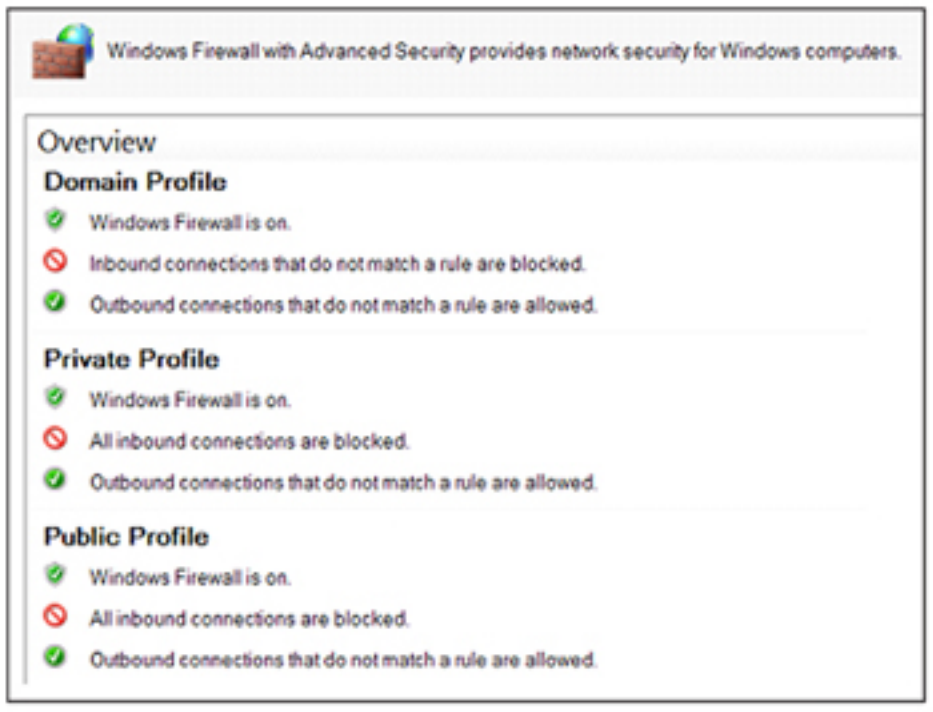


FIGURE 14 - WINDOWS FIREWALL RECOMMENDED CONFIGURATIONS

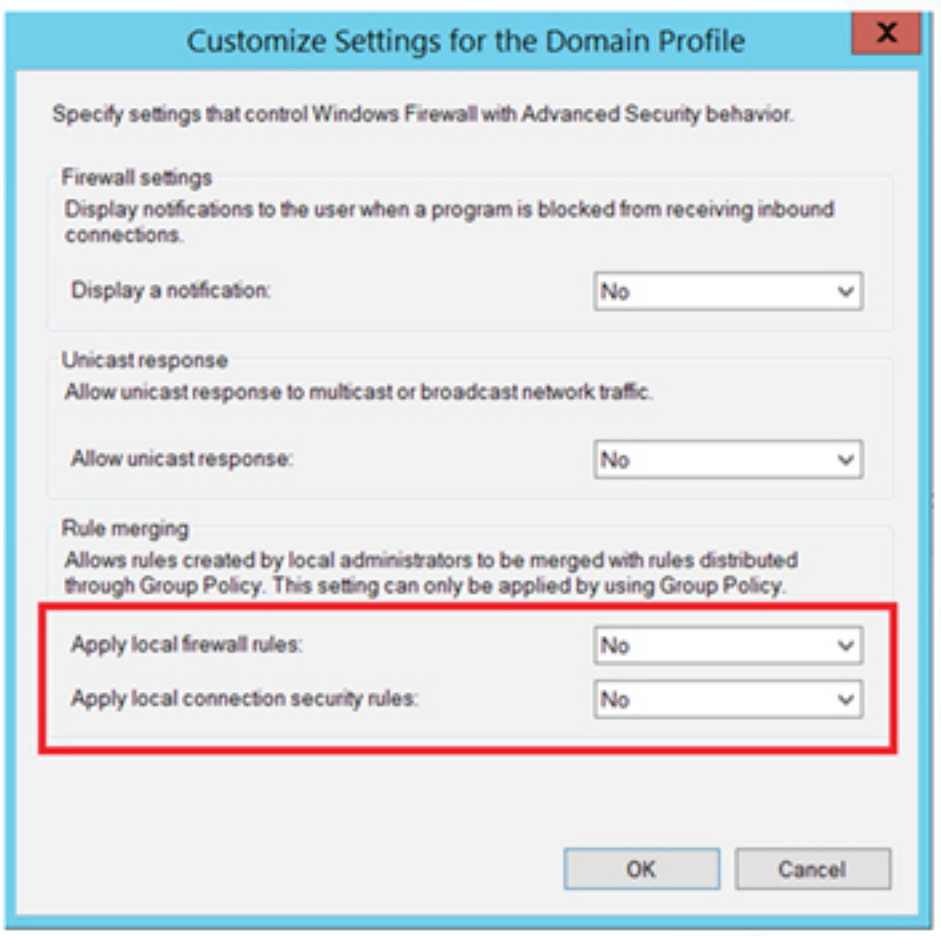


FIGURE 15 - WINDOWS FIREWALL DOMAIN PROFILE CUSTOMIZED SETTINGS

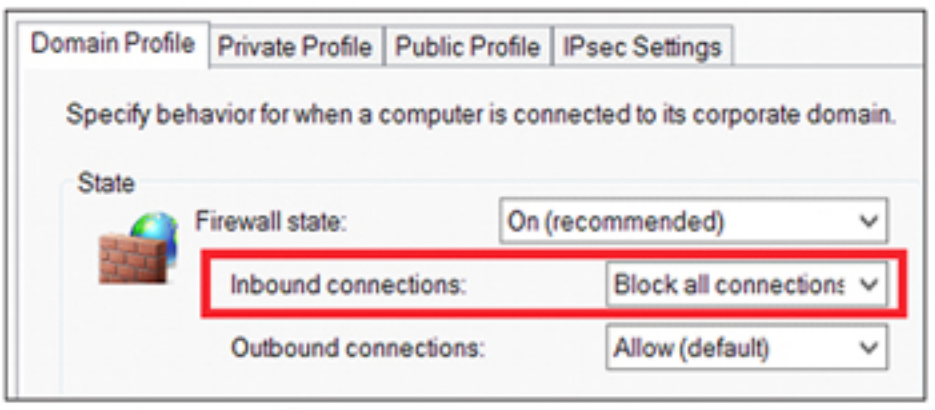


FIGURE 16 - WINDOWS FIREWALL - "BLOCK ALL CONNECTIONS" SETTINGS

PROTOCOL / PORT	WINDOWS FIREWALL RULE	COMMAND LINE ENFORCEMENT
SMB TCP/445, TCP/139, TCP/135	Predefined Rule: File and Print Sharing	netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no
REMOTE DESKTOP PROTOCOL TCP/3389	Predefined Rule: Remote Desktop	netsh advfirewall firewall set rule group="Remote Desktop" new enable=no
WMI	Predefined Rule: Windows Management Instrumentation (WMI)	netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=no
WINDOWS REMOTE MANAGEMENT / POWERSHELL REMOTING TCP/80, TCP/5985, TCP/5986	Predefined Rule: Windows Remote Management Windows Remote Management (Compatibility) Port Rule: 5986	netsh advfirewall firewall set rule group="Windows Remote Management" new enable=no Via PowerShell: Disable-PSRemoting -Force

FIGURE 17 - WINDOWS FIREWALL SUGGESTED BLOCK RULES

Name	Group	Profile	Enabled	Action
WinRm via HTTPs - Block Inbound		All	Yes	Block
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (Spooler Service - RPC-EPM...	File and Printer Sharing	All	Yes	Block
Remote Desktop - Shadow (TCP-In)	Remote Desktop	All	Yes	Block
Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	Yes	Block
Remote Desktop - User Mode (UDP-In)	Remote Desktop	All	Yes	Block
Windows Management Instrumentation (ASync-In)	Windows Managemen...	All	Yes	Block
Windows Management Instrumentation (DCOM-In)	Windows Managemen...	All	Yes	Block
Windows Management Instrumentation (WMI-In)	Windows Managemen...	All	Yes	Block
Windows Remote Management (HTTP-In)	Windows Remote Ma...	All	Yes	Block
Windows Remote Management (HTTP-In)	Windows Remote Ma...	All	Yes	Block

FIGURE 18 - WINDOWS FIREWALL SUGGESTED RULE BLOCKS VIA GROUP POLICY

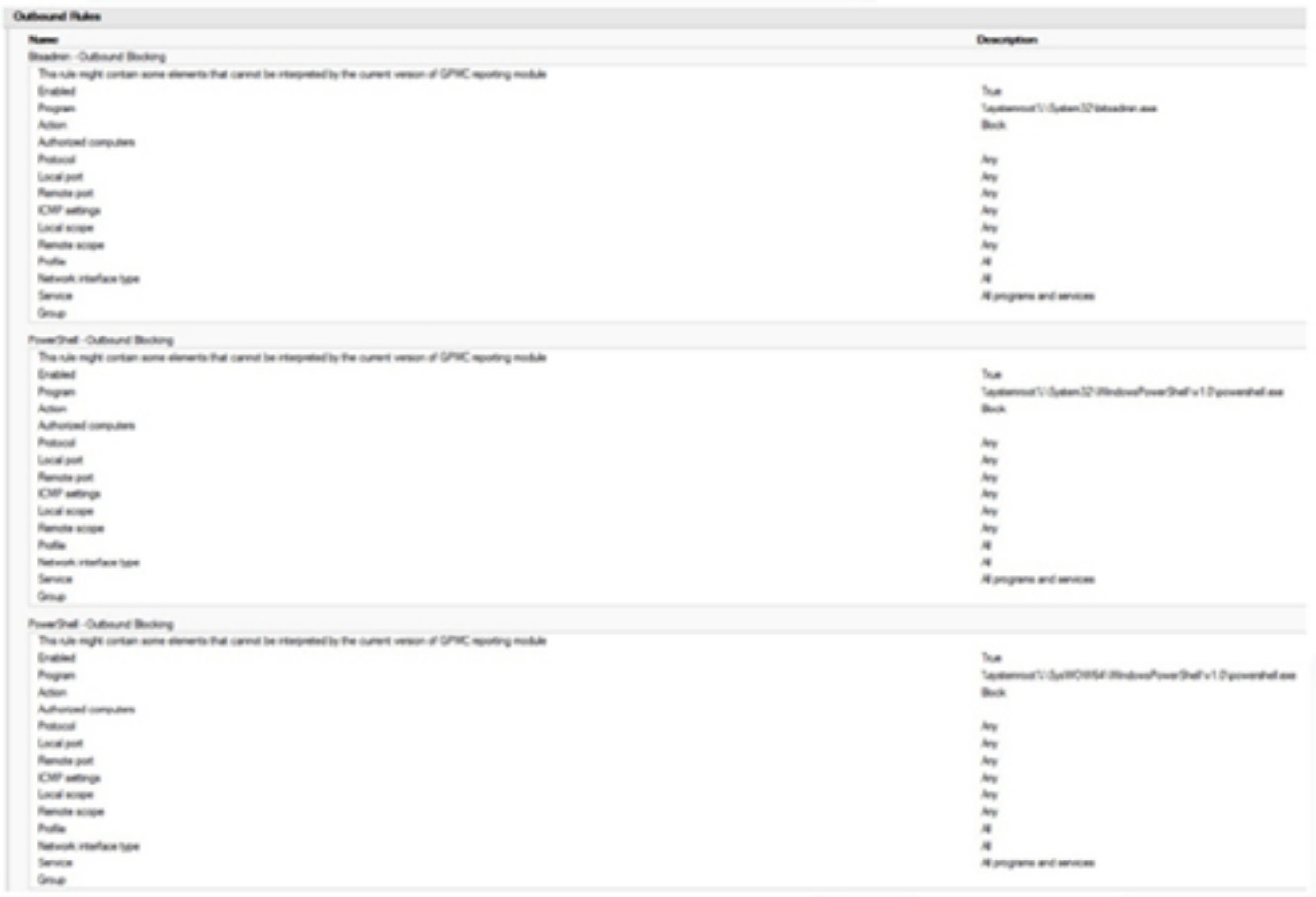


FIGURE 19 - WINDOWS FIREWALL RULE EXAMPLE TO BLOCK SPECIFIC BINARIES FROM MAKING ENDPOINT OUTBOUND CONNECTIONS

In addition, the dynamic storage of cleartext passwords in memory to support authentication should be disabled on all endpoints. While this facility is disabled by default on newer versions of Windows, older versions may still permit the use of cleartext passwords. Sophisticated malware can have the capability to scan dynamic memory and recognize temporary storage of credential details.

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential
REG_DWORD = “0”

FIGURE 20 - REGISTRY KEY AND VALUE FOR DISABLING WDIGEST AUTHENTICATION

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\TokenLeakDetectDelaySecsREG_DWORD = “30”

FIGURE 21 - REGISTRY KEY AND VALUE FOR ENFORCING THE"TOKEN LEAK DETECT DELAY SECS" SETTING TO CLEAR CREDENTIALS IN MEMORY OF LOGGED OFF USERS AFTER 30 SECONDS

Setting	State	Comment
Configure SMB v1 server	Not configured	No
Configure SMB v1 client driver	Not configured	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Not configured	No
Extended Protection for LDAP Authentication (Domain Controllers only)	Not configured	No
Turn on Windows Defender protection against Potentially Unwanted Applications (DEPRECATED)	Not configured	No
Enable Structured Exception Handling Overwrite Protection (SEHOP)	Not configured	No
Apply UAC restrictions to local accounts on network logons	Not configured	No
WDigest Authentication (disabling may require KB2871997)	Disabled	No
Lsass.exe audit mode	Not configured	No
LSA Protection	Not configured	No
Remove "Run As Different User" from context menus	Not configured	No
Block Flash activation in Office documents	Not configured	No

FIGURE 22 - DISABLING WDIGEST AUTHENTICATION VIA THE “MS SECURITY GUIDE" GROUP POLICY TEMPLATE

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Credssp\PolicyDefaults

FIGURE 23 - ADDITIONAL REGISTRY KEY FOR HARDENING AGAINST CLEARTEXT PASSWORD STORAGE

CONNECTIVITY HARDENING

The Remote Desktop Protocol (RDP) is frequently exploited by malware to gain a foothold in systems and effect lateral movement to escalate privileges to the point where ransomware can be installed and executed. RDP utilized TCP Port 3389 for internet traffic. As for SMB, regular scanning of all public IP addresses for this open port can help minimize the ability of attackers to use RDP to attack a system.

Where internet access for communications such as RDP or SMB is required, system configurations should be hardened to restrict access to a limited set of pre-authorized IP addresses. Connection mechanisms should also implement reasonable security practices such as multi-factor authentication to prevent a compromised remote system from being used as a platform to launch a remote attack.

RDP connections should also implement Network Level Authentication (NLA) to require any connecting user to authenticate their access credentials before establishing an external connection.

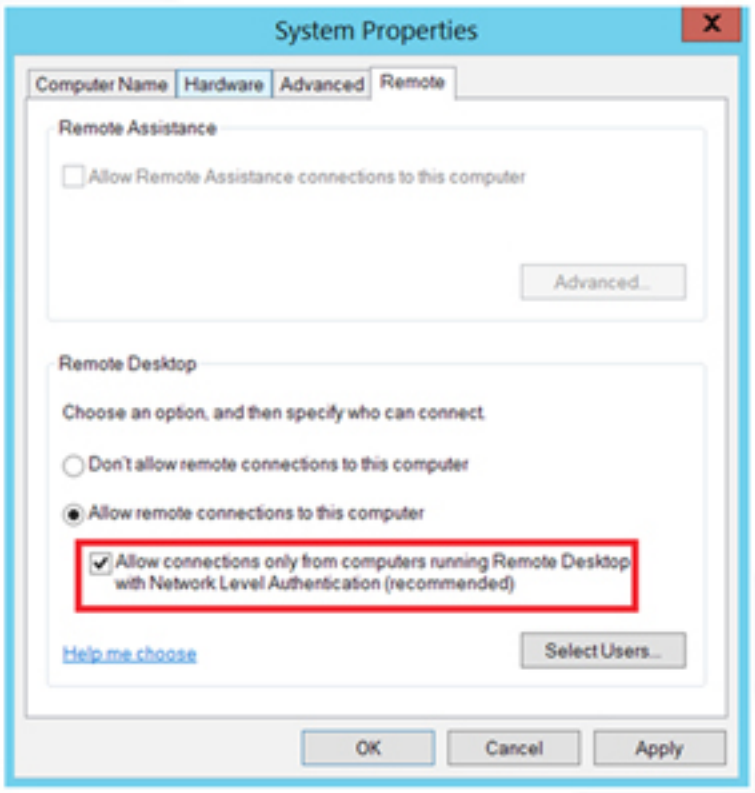


FIGURE 24 - ENABLING NLA VIA THE UI

Setting	State	Comment
Server authentication certificate template	Not configured	No
Set client connection encryption level	Not configured	No
Always prompt for password upon connection	Not configured	No
Require secure RPC communication	Not configured	No
Require use of specific security layer for remote (RDP) connections	Not configured	No
Do not allow local administrators to customize permissions	Not configured	No
Require user authentication for remote connections by using Network Level Authentication	Enabled	No

FIGURE 25 - ENABLING NLA VIA GROUP POLICY

Local Policies/User Rights Assignment

Policy	Setting
Deny access to this computer from the network	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a batch job	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a service	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on locally	MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on through Terminal Services	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts

FIGURE 26 - GROUP POLICY CONFIGURATION FOR RESTRICTING HIGHLY PRIVILEGED DOMAIN AND LOCAL ADMINISTRATIVE ACCOUNTS FROM LEVERAGING RDP

ENDPOINT HARDENING

A typical endpoint weakness is the presence of local administrator accounts, often using the same username and password on each endpoint. This practice provides an exploitable vulnerability that enables ransomware to be quickly spread across endpoints with minimum effort.Therefore, endpoint configuration should prevent local administration accounts from accessing networks or remote terminal services or logging on a service, batch job, or any other process that can be used for privilege escalation and propagation of malware.

Account policies should also prevent the reuse of passwords for any account, with minimum complexity rules based on the privileges afforded to an account. Use of the Microsoft Local Administrator Password Solutions (LAPS) tool can be used for enforcing rules and audit systems to ensure compliance and identify weaknesses.

Local Policies/User Rights Assignment

Policy	Setting
Deny access to this computer from the network	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a batch job	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a service	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on locally	MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on through Terminal Services	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts

FIGURE 27 - EXAMPLE OF PRIVILEGED ACCOUNT ACCESS RESTRICTIONS FOR A STANDARD WORKSTATION USING GROUP POLICY SETTINGS

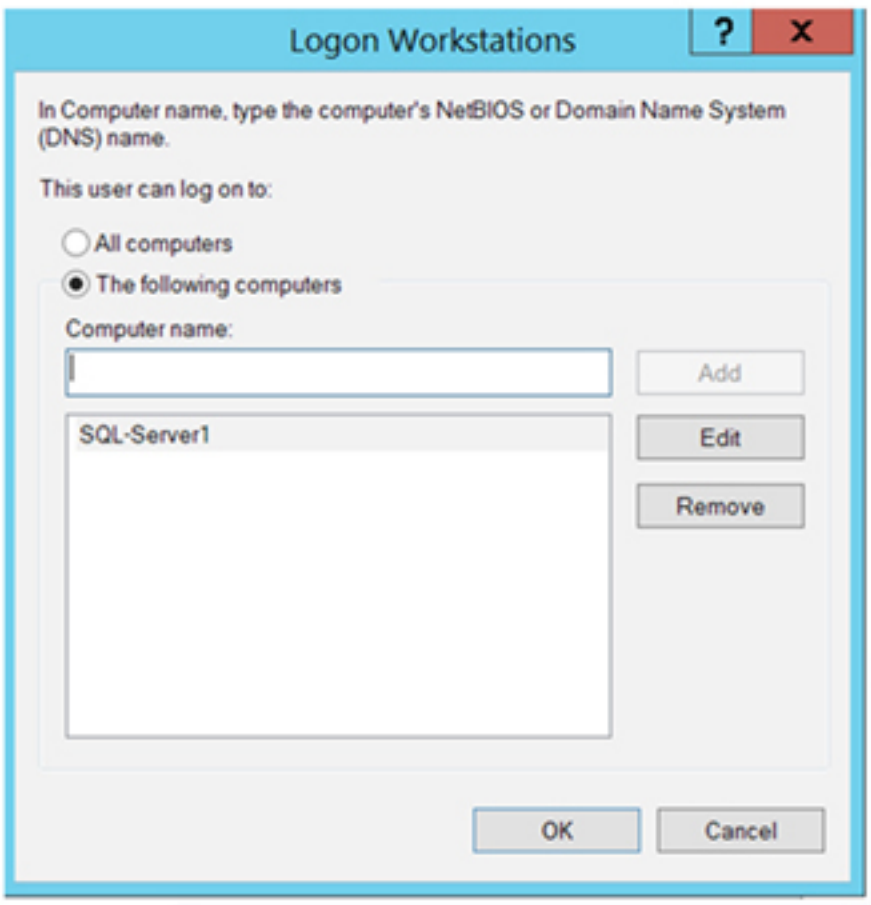


FIGURE 28 - OPTION TO RESTRICT AN ACCOUNT TO LOGON TO SPECIFIC ENDPOINTS

ADMINISTRATION ACCESS CONTROLS

Another simple technique to reduce the opportunities for attackers to compromise systems is to impose restrictions on accounts with elevated access permissions. A standard method is the use of Privileged Access Workstations (PAWS) that have limited system access through the partitioning of networks using virtual networks. Only designated endpoint devices may be used for administration, and these endpoints reside within a virtual network, with no access outside of the boundary of this network. Administration accounts should be explicitly prevented from accessing other endpoints to avoid exploitation in attacks.

SERVICE ACCOUNT ACCESS CONTROLS

Where service accounts exist in domain-based systems, it is recommended that the access permissions be restricted to prevent their use for remote desktop access or network-based logons to limit the potential damage should a service account become compromised. In addition, the principle of least privilege should apply to such accounts to prevent their use as an attack vector.

Any endpoint with no requirement for service account access should be configured to prevent access by such accounts explicitly.

PROTECTED USERS SECURITY GROUPS

Organizations should consider implementing Microsoft's "Protected Users" security group for all accounts with privileged access permissions to increase protection from malicious use of compromised accounts.

INCIDENT RESPONSE

If an active ransomware attack is suspected or detected, mitigation measures can be taken to halt the attack without shutting down systems. For example, for a windows-based system, a straight forward step is to apply temporary configuration changes to the Windows Firewall policy to stop communications associated with ransomware command and control activities. Additionally, restricting traffic from endpoints to the internet can halt a ransomware attack. Typical restrictions include:

- TCP Ports 135, 139, and 445 are used by SMB traffic for file and print sharing.
- TCP Port 3389 is used by RDP traffic for remote management.
- TCP Ports 80, 5985, and 5986 are used by Windows Remote Management and Remote PowerShell traffic.
- TCP Ports are assigned dynamically by Windows Management Instrumentation (WMI) and Distributed Component Object Model (DCOM).

An alternative method for preventing ransomware from exploiting SMB and RDP traffic is to disable all relevant traffic on endpoints with a simple PowerShell command or through changes to the registry.

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

FIGURE 29 - POWERSHELL COMMAND TO DISABLE SMB V1

HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
Registry entry: SMB1
REG_DWORD = "0" (Disabled)

FIGURE 30 - REGISTRY KEY AND VALUE FOR DISABLING SMB V1 SERVER (LISTENER)

HKLM\SYSTEM\CurrentControlSet\services\mrxsmb10
Registry entry: Start

REG_DWORD = "4" (Disabled)
HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation
Registry entry: DependOnService

REG_MULTI_SZ: "Bowser","MRxSmb20","NSI"

FIGURE 31 - REGISTRY KEYS AND VALUES FOR DISABLING SMB V1 CLIENT

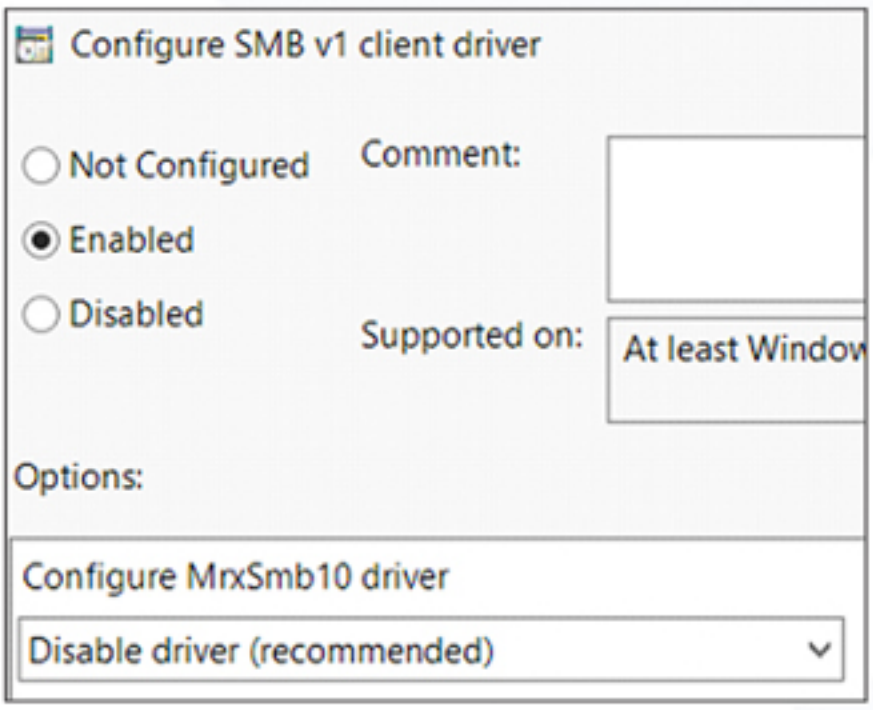
Setting	State	Comment
Configure SMB v1 server	Disabled	No
Configure SMB v1 client driver	Enabled	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Enabled	No

- ComputerConfiguration>Policies>AdministrativeTemplates>MSSecurityGuide>ConfigureSMBv1ClientDriver
  - Enabled
- ConfigureMrxSMB10driver
  - Disabledriver

FIGURE 32 - DISABLING SMB V1 SERVER VIA THE "MS SECURITY GUIDE" GROUP POLICY TEMPLATE

Setting	State	Comment
Configure SMB v1 server	Disabled	No
Configure SMB v1 client driver	Enabled	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Enabled	No

FIGURE 33 - DISABLING SMB V1 CLIENT DRIVER VIA THE "MS SECURITY GUIDE" GROUP POLICY TEMPLATE



- ComputerConfiguration >Policies> AdministrativeTemplates> MSSecurityGuide> ConfigureSMBv1Client (extrasettingneededforpre-Win8.1/2012R2)
  - Enabled
- ConfigureLanmanWorkstationDependencies
  - Bowser
  - MrxSMB20
  - NSI

FIGURE 34 - DISABLING SMB V1 CLIENT DRIVER VIA THE "MS SECURITY GUIDE" GROUP POLICY TEMPLATE – ADDITIONAL SETTING

Setting	State	Comment
Configure SMB v1 server	Disabled	No
Configure SMB v1 client driver	Enabled	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Enabled	No

FIGURE 35 - DISABLING SMB V1 CLIENT EXTRA SETTINGS VIA THE "MS SECURITY GUIDE" GROUP POLICY TEMPLATE

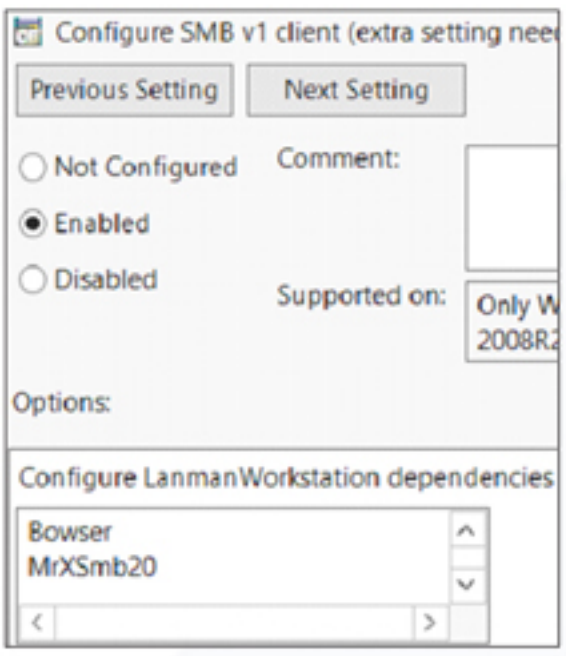


FIGURE 36 - DISABLING SMB V1 CLIENT DRIVER VIA THE "MS SECURITY GUIDE" GROUP POLICY TEMPLATE– ADDITIONAL SETTINGS ENSURING THAT THE "MRXSMB10" OPTION IS NOT PRESENT

A common tactic for ransomware to spread is using administrative or hidden network shares to effect lateral movement through a system. Disabling all administrative and hidden shares on endpoint devices can provide a temporary measure to halt the spread of ransomware across endpoints. However, the operational functionality of the system will potentially be impacted while this measure is in place and the ransomware is removed from the system. The impact is particularly significant in a domain-based environment.

- HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters DWORD Name = "AutoShareWks"
  Value = "0"

FIGURE 37 - REGISTRY VALUE FOR DISABLING ADMINISTRATIVE SHARES ON WORKSTATIONS

- HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters DWORD Name = "AutoShareServer"
  Value = "0"

FIGURE 38 - REGISTRY VALUE FOR DISABLING ADMINISTRATIVE SHARES ON SERVERS

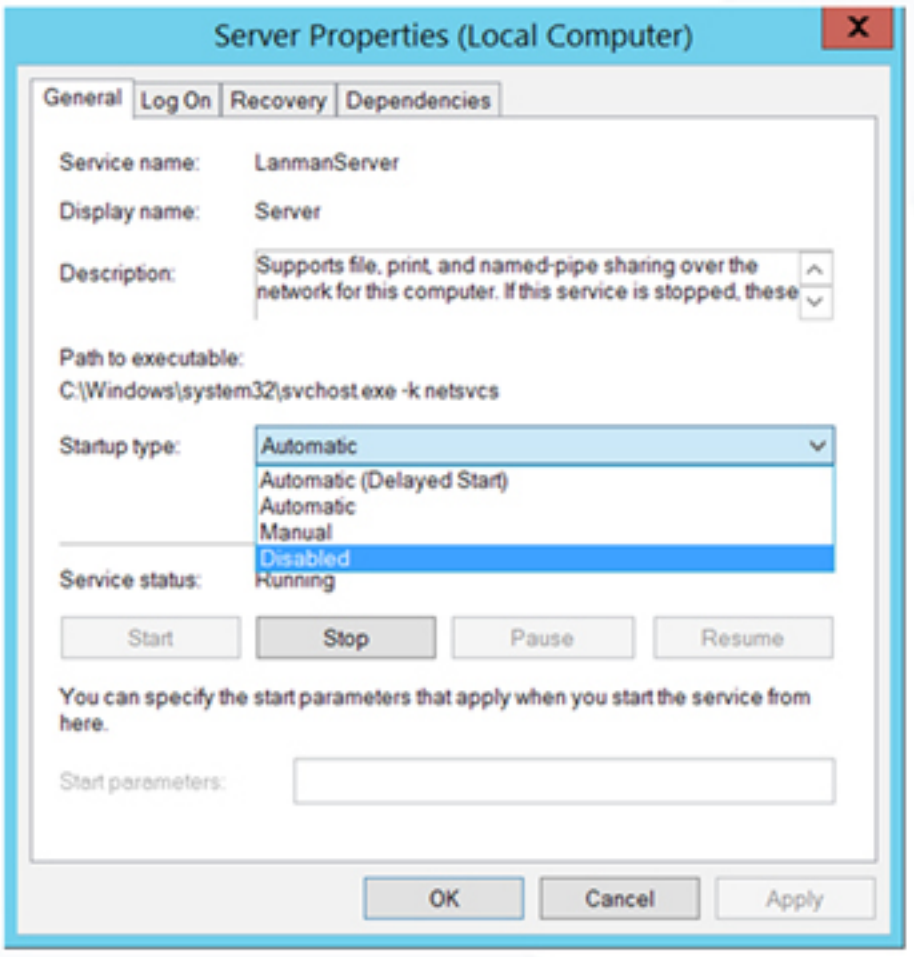


FIGURE 39 - "SERVER" SERVICE PROPERTIES

Setting	State	Comment
MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	Not configured	No
MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended e...	Not configured	No
MSS: (AutoShareServer) Enable Administrative Shares (recommended except for highly secure envi...	Disabled	No
MSS: (AutoShareWks) Enable Administrative Shares (recommended except for highly secure enviro...	Disabled	No

FIGURE 40 - DISABLING ADMINISTRATIVE AND HIDDEN SHARES VIA THE "MSS (LEGACY)" GROUP POLICY TEMPLATE

RECOVERY ADVICE

SYSTEM BACKUPS

Recovery from a ransomware attack requires access to backups that predate the infection of the system. Creating a storage volume supplemented with archival differential-based file backups offers the most effective approach.

The backup data must be isolated from the business systems such that ransomware infecting the system cannot compromise the backup data, rendering it useless. Air-gapping the backup storage medium from the system as soon as the backup is taken will provide an effective mechanism.

As ransomware becomes more sophisticated, persistent attacks are being seen where the malware attacks and compromises backups for a period before the launch of the active encryption phase of the attack. As a result, organizations that do not regularly test backups may find that the integrity of the stored data was compromised during the backup process. Consequently, a significant volume of data may be lost, depending on the period between the initial malware infection and the start of the ransomware encryption process.

Also, the differential backups must be performed sufficiently frequently such that the volume of changed data lost in the period from the backup being taken to the system requiring restoration is minimized.

ZERO TRUST ARCHITECTURES

AN ALTERNATIVE APPROACH

The move towards implementing systems using a Zero Trust Architecture is seen as a necessary long-term solution for combatting threats from increasingly sophisticated and persistent ransomware threats. In addition, the US government has published a strategy for the migration of vital US Government systems to improve protection.

A Zero Trust Architecture is a significant change in mindset when implementing and managing security controls. This approach goes beyond changes to network design and requires a considerable investment of resources and effort. However, this is seen as a step-change in security posture to counter the deployment of sophisticated attack vectors.

Traditionally, IT systems implemented security controls on the boundary between the internal network and the internet-connected outside world, focusing on blocking unauthorized access. However, once an attacker made their way inside the perimeter, the security controls they faced moved from active access management to more passive monitoring techniques.

As a result, once inside the system, the attacker could exploit further weaknesses to reconnoiter the network, uncover vulnerabilities, and escalate privileges and hide their presence.

In a Zero Trust Architecture, there is no assumption of trust anywhere in a system, inside or outside boundaries. Instead, trust must be earned at every step, with each user and service requesting access assumed suspect until proven legitimate. The security of the network then depends on the use of robust authentication techniques for each interaction.

The effectiveness of security controls depends on the network design being complete and fully defined for all systems, services, devices, and users. Any error or omission in the definition can lead to access issues for legitimate users and weaknesses in security controls. Therefore, this approach is dependent on a robust definition of all devices and users if the network is to operate efficiently with minimum vulnerabilities. This dependency places a significant emphasis on the skills and knowledge of the network designers to get right.

The process of establishing trust depends on monitoring and inspecting transactions to build confidence in the communications between a device or user and a service. The system builds up a picture of the trustworthiness and uses the results to determine whether or not to grant or deny access. Decisions to establish trust within the system are made for every interaction on a case-by-case basis throughout the network. This approach is significantly different from traditional methods where trust-based decisions are concentrated at the boundaries, typically made by a firewall or a VPN connection.

Zero Trust is built around the principle of least privilege. This philosophy ensures authorized users are only allowed access to those services and specific data necessary for the performance of their duties.Furthermore, it is egalitarian in that all users and services are equally treated as untrusted.

Implementing Zero Trust requires continuous monitoring of services and devices. Detecting operational health issues or suspicious activities feeds into the trust criteria upon which access decisions are made.

ZERO TRUST POLICIES

The Zero Trust model operates by applying a policy decision to every action a user or device performs that determines if the activity will be permitted. These checks encompass every access attempt to services, resources, or data. If the policy criteria applied to the instigator of the action for the specific type of action are not met, the action is blocked, and a security event is reported. This approach provides significant challenges for an attacker within a system looking to exploit weaknesses to propagate and execute ransomware.

Zero trust policies provide a means for ensuring that only authorized users and devices are granted access to those services and data they are explicitly permitted to access.

Each policy is composed of a set of rules that are applied to access requests from users or devices that meet defined criteria. The assessment of compliance with the rules results in an assignment of action to that access request.

The power of Zero Trust is that rules and criteria can be dynamic, changing in response to threat intelligence or analysis of the previous behavior. For example, a suspicious user may suddenly find their access restricted until they can demonstrate their legitimacy. Likewise, recognizing the detected behavior of services that match behaviors seen in previous attacks can be used to trigger a security response.

LMNTRIX'S PROTECTION AND CONTAINMENT STRATEGIES

LMNTRIX STRATEGY

LMNTRIX's approach to ransomware follows the highly regarded NIST cybersecurity framework , developed for assessing and improving their ability to protect, detect and respond to cyber incidents. Established to manage cybersecurity risks, it provides a robust foundation for protecting businesses from the threat of ransomware attacks.

IDENTIFY

Protection from ransomware attacks starts with identifying risks to physical and logical assets, be that data, services, personnel, or equipment. Having a complete understanding of a business's infrastructure, networks, connections, and dependencies will lead to a definitive set of known and credible risks that LMNTRIX's services can manage.

PROTECT

The protection of critical assets requires the implementation of effective security controls that are thorough enough to reduce risks to an acceptable level while remaining proportionate to the business's needs. In addition, the protection services are intended to prevent attacks from gaining a foothold or limit and contain any attacks penetrating outer defenses.

The most effective protection comes from a multi-layered approach that provides strength in depth, with vulnerabilities in any one layer protected against exploitation by other functionally independent layers. Technical controls can balance inherent weaknesses in the human element of security. Diversity in product manufacturers can reduce the chance that multiple devices have the same common vulnerability.

DETECT

While most businesses focus their resources on protection, the increasing sophistication of attacks means that it is inevitable that defenses will be breached. Companies need to be prepared for this eventuality. Processes and monitoring equipment provides the mechanisms for the detection of ransomware attacks. Detection of an attack before activation of ransomware code can stop an attack in its tracks. Early detection of an activated attack will limit the impact and facilitate fast recovery.

LMNTRIX Detect services provide organizations with advanced detection capabilities to detect sophisticated, persistent threats and provide protection to halt such attacks before they can gain a foothold. By combining constant monitoring with detection capabilities informed by intelligence lead threat prediction, these services offer effective control for capable attacks.

RESPOND

Planned processes to react and respond to a ransomware attack will limit the effects, constrain the attack's ability to be sustained and restrict its ability to move laterally through systems or across supply chain boundaries. An effective response plan will contain and mitigate an ongoing attack, identify the exploited vulnerabilities and patch these to halt the attack. Additionally, the prompt removal of malware and counterattack of command and control mechanisms will support the ransomware response measures.

Investigative processes will precisely determine the attacker's actions to reverse any changes and notify affected parties, internal or external, of any compromised assets along with necessary recovery measures. Additionally, the **LMNTRIX** Respond service can help organizations stop the attack in its tracks, and the associated Threat Hunting and Reconnaissance services detect any consequential security impact.

RECOVER

Plans and processes for the recovery of compromised services will rapidly restore services with minimized business impact. A pre-planned preparation for recovery with tried and tested techniques can save a business from a potentially catastrophic attack.

LMNTRIX SERVICES

LMNTRIX's advanced threat detection and response capabilities offer clients an effective solution to counter the latest sophisticated and persistent ransomware threats. The **LMNTRIX** Respond endpoint agent blocks malware and ransomware while the rest of its service stack offers tailored detection and response capabilities. The services detect ransomware at the earliest execution stage to minimize impact before the malware gets a foothold in compromised systems.

LMNTRIX's global network of Cyber Defense Centers (CDC) is on hand to provide continuous monitoring and investigation services around the clock. Teams of highly trained and certified intrusion analysts provide constant vigilance and on-demand network analysis. Intrusion analysts monitor networks and endpoints to detect the earliest signs of compromise using intelligence-led detection methodologies. Any detected potential compromise is analyzed to confirm the breach, minimizing the impact of a false positive detection. In addition, continuous threat hunting processes look for advanced malicious activity that traditional alerting mechanisms cannot identify.

Intrusion analysts leverage deceptions and multi-threat network detection to investigate, classify, and analyze risks in real-time using advanced forensic capabilities. Additionally, active validated incidents are afforded high-touch management and incident support, tailored to each client and coordinated by a designated investigation manager.

For effective ransomware protection, endpoint containment features provide immediate reaction to imminent data theft or lateral movement. Affected hosts are quarantined to reduce or eliminate the consequences of any ongoing breach.

Once an attack is confirmed, a rapid breach investigation is initiated to re-secure networks, remediate technical damage, and assess potential business impact. **LMNTRIX's** CDC-based expert incident responders can provide remote investigation, supported with an onsite incident response using local certified partners if necessary.

The response capability will reverse the ransomware, identifying the source of infection and eradicating it out of the network. A constant containment process then counters the follow-up attacks and re-infection attempts that persistent attackers employ as part of the typical multi-pronged and sustained attack.

To provide maximum flexibility and adaptability, clients can select from a range of discrete services to create a bespoke consolidated service that meets their individual needs in a proportionate and cost-effective package.

LMNTRIX INTELLIGENCE

The fundamental strategy for tackling advanced persistent ransomware threats is the use of intelligence to detect an attack before it has gained a foothold or caused disruption. The **LMNTRIX** Intelligence service provides organizations with access to threat intelligence information in a form that can be used effectively.

LMNTRIX Intelligence aggregates information from over three hundred threat intelligence sources and has been built with the capability to aggregate thousands more in the future. The proprietary technology behind **LMNTRIX** Intelligence provides clients with access to earlier detection and identification of adversaries. This service allows attack protection measures to be taken to halt an attack before it causes harm. In addition, the service correlates over 650 million threat indicators against real-time network data, a capability that is beyond most organizations.

This approach enables detection at every point along the attack lifecycle, making it possible to mitigate threats before material damage to a targeted organization has occurred.

LMNTRIX DECEIVE

The **LMNTRIX** Deceive service help prevent ransomware from gaining a foothold in your systems by creating a mirror of your network that presents the attackers with misleading and deceptive data that creates confusion and halts their attack.

Decoys are deployed across the network that serves as an early warning system of potential ransomware activity. The tripping of a decoy by any ransomware attempting to move laterally can provide the first indication that an attack is in progress. In addition, deceptive files known as tags that are deployed on every endpoint provide another early warning system as they are tripped once ransomware tries to encrypt them. These features enable the detect and respond services to be engaged before the ransomware can gain a foothold on the live network.

This service also has the advantage of providing a reliable indicator that your networks are being probed as a ransomware attack precursor. No legitimate users will interact with the mirrored environment, so any monitored activity can be attributed directly to an attack. Additionally, this feature enables the detect and protect services on the live network to be preempted and prewarned of the in-progress attack, significantly enhancing their responsiveness and effectiveness if the attackers migrate from the deceptive mirror to the live network.

LMNTRIX DETECT

The **LMNTRIX** Detect service uses a proprietary network sensor that delivers integrated, multi-layer detect-in-depth capability for identifying a ransomware attack. The sensor has ability to detect both known and unknown threats across an entire network and delivers more comprehensive detection capabilities than traditional detection services.

Ransomware detection before an attack is instigated will provide robust protection. Identifying the initial attack vector and preventing malware propagation and exfiltration of sensitive data is essential for protecting systems. **LMNTRIX** Detect service has the capability to identify and halt attacks before they can get established and cause harm.

Email and Web sandbox capabilities enable the detection and containment of ransomware pre-execution. This feature provides the opportunity to halt an attack if the ransomware code cannot move outside the sandbox.

Typical characteristics of attacks include using Bots (automated software programs known as robots) and access to specific web addresses or Uniform Resource Locators (URL) controlled by the attackers.This service canmonitor for Intrusions, Malware, Bot, URL, ransomware and command and control activity. Additionally, this facility enables the detection of ransomware post-execution.

LMNTRIX RESPOND

The **LMNTRIX** Respond service combines Endpoint Detection and Response (EDR) services with Next-Generation Antivirus (NGAV) to provide enhanced ransomware protection capabilities. A light weight custom agent is deployed on all endpoints to capture detailed state information and protect against ransomware attacks. Specifically, it can protect against exploits, malware, file-less attacks, malware-less attacks, phishing, injection, macro-based attacks, ransomware, credential theft, and adversary tradecraft.

The **LMNTRIX** CDC uses the agent to monitor all endpoint activity continuously, conduct adversary hunting, validate breaches, investigate, contain, remediate and detect encrypted attacks. Using a lightweight sensor allows intrusion analysts to delve deep into the inner workings of endpoints and expose anomalous behaviors. This capability uses advanced monitoring and analysis techniques, including live memory analysis, direct physical disk inspection, network traffic analysis, and endpoint state assessment. This service is not constrained by the use of predefined signatures or rules. Instead, it leverages unique endpoint behavioral monitoring and advanced machine learning to thoroughly examine endpoint behavior to analyze better and identify zero-days and hidden threats that other endpoint security solutions will miss. This information enables intrusion analysts to instantly find similarly infected endpoints and quickly expand their visibility into the full scope of a compromise. Once an intrusion is confirmed, the malware-driven tactics, techniques, and procedures (TTP) are disrupted. The attacker's lateral movement is limited by quarantining and blocking the threat.

LMNTRIX HUNT

The **LMNTRIX** Hunt service delivers extensive visibility, high-performance threat hunting, and unrivaled incident response by augmenting the Hunt Team's capabilities with Behavior and Analytics technology. For situations where automated ransom detection techniques are not effective, the **LMNTRIX** Hunt service can be employed to detect the initial signs of a ransomware attack footprint on a network and eradicate it.

This technology also provides a photographic memory of networks. Snapshots with full-fidelity packet capture, optimized and stored for up to a year, will demonstrate with absolute certainty if a ransomware attack has adversely impacted your systems.

Capturing and retaining network activity (packets) provides the ability to go back in time to see historical activity. This capability enables the **LMNTRIX** Hunt post-breach forensics capability to conduct exhaustive post-infection analysis to determine how ransomware entered a system, how it propagated, and what damage it caused. In addition, the data will show what data was accessed and how it was exfiltrated.

LMNTRIX Hunt detects threats in real-time and automatically replays stored packets to discover previously unknown threats through the correlation of proprietary research intelligence, machine learning, flow-based traffic algorithms, and multiple third-party threat intelligence feeds.

The Threat Hunting service involves the proactive, stealthy, and methodical pursuit and eviction of adversaries inside networks without relying on finding compromise indicators. A team of intrusion analysts and threat hunters monitor networks and endpoints around the clock, applying the latest intelligence and proprietary methodologies to look for signs of compromise. Once a potential compromise is detected, in-depth analysis of affected systems is performed to confirm the attack and begin mitigation measures rapidly.

LMNTRIX RECON

LMNTRIX Recon is a proactive defense measure that searches for evidence that your business may be the target for a planned ransomware attack. It will also detect if data stolen from your networks has been exfiltrated and offered for sale on the dark web.

By leveraging intelligence and employing proprietary technology, **LMNTRIX's** Recon service follows activity on the dark web. This service includes monitoring the online conversations of attackers discussing potential targets or seeking specific information about business systems. This provides an advanced warning of possible exploit attempts and the probable attack vectors that will be employed. This valuable information can be used to detect attacks before they gain a foothold, allowing the detection and response services.

Monitoring online conversations is also a valuable technique for confirming a breach has occurred by looking for ransomware gangs bragging about successes and sharing samples on the dark web. This technique allows the identification of the perpetrators and the type of ransomware code that was deployed. Our technical specialists will seek to gain a copy of the ransomware code and employ reverse engineering techniques to discover how it enters, propagates around target networks, and look for flaws in code to halt the ransomware, while neutralizing any adverse impact..

LMNTRIX
BE THE HUNTER | NOT THE PREY

ABOUT **LMNTRIX**

LMNTRIX is the leader in intelligence led security-as-a-service. Working as a seamless, scalable extension of customer security operations, **LMNTRIX** offers a single MDR solution called Active Defense that blends our cyber defense platform called **LMNTRIX** XDR with innovative security technologies, nation-state grade threat intelligence and world-renowned Cyber Defence Centers. With this approach, **LMNTRIX** eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyberattacks. Our service differentiators include:

LMNTRIX XDR natively unifies Machine and Underground Intelligence, NGAV, EDR, NDR, Network Forensics, UEBA and Deception Everywhere with completely automated attack validation, investigation, containment, and remediation on a single, intuitive platform.

LMNTRIX Tech Stack is a powerful proprietary threat detection stack that is deployed onsite, behind existing controls. It's made up of network sensors, endpoint agents and deceptions everywhere. It combines multiple threat detection systems, with machine learning, threat intel, correlation, static file analysis, heuristics, and behavior and anomaly detection techniques to find threats in real-time. It decreases alarm fatigue by automatically determining which alerts should be elevated to security events, and reduces false positives by requiring consensus across detection.

LMNTRIX Cyber Defense Centers - A global network of cyber defense centers that are complemented by our local partner SOCs, with highly trained and certified intrusion analysts who provide constant vigilance and on-demand analysis of your networks. Our intrusion analysts monitor your networks and endpoints 24x7, applying the latest intelligence and proprietary methodologies to look for signs of compromise. When a potential compromise is detected, the team performs an in- depth analysis on affected systems to confirm the breach. When data theft or lateral movement is imminent, our endpoint containment feature makes immediate reaction possible by quarantining affected hosts, whether they are on or off your corporate network while our automated network containment feature blocks the threat traversing your Firewalls or through our integration with cloud security solutions such as Zscaler, Netskope and Cisco Umbrella. This significantly reduces or eliminates the consequences of a breach.

TO LEARN MORE ABOUT **LMNTRIX** VISIT

https://lmntrix.com/

LMNTRIX USA.
333 City Blvd West, 18th Floor,
Suite 1805, Orange, CA 92868
+1.888.958.4555

LMNTRIX UK.
200 Brook Drive, Green Park,
Reading, RG2 6UB
+44.808.164.9442

LMNTRIX SINGAPORE.
60 KAKI BUKIT PLACE#05-19
EUNOS TECHPARK
+65 3159 0639

LMNTRIX Hong Kong.
14F, Manning House, 38-48
Queen's Road Central, Central,
Hong Kong
+852.580.885.33

LMNTRIX Australia.
Level 32, 101 Miller Street,
North Sydney NSW 2060,
+61.288.805.198